LANTRONIX®

SecureLinx™ Management Appliance

User Guide

Part No. 900-386
Rev.F November 2007

Copyright & Trademark

© 2005, 2006, 2007 Lantronix. All rights reserved. No part of the contents of this book may be transmitted or reproduced in any form or by any means without the written permission of Lantronix. Printed in the United States of America.

Ethernet is a trademark of XEROX Corporation. UNIX is a registered trademark of The Open Group. Windows 95, Windows 98, Windows 2000, Windows NT, and Windows XP are trademarks of Microsoft Corporation. Netscape is a trademark of Netscape Communications Corporation.

Open Source Software

Some applications are Open Source software licensed under the Berkeley Software Distribution (BSD) license or the GNU General Public License (GPL) as published by the Free Software Foundation (FSF). Redistribution or incorporation of BSD or GPL licensed software into hosts other than this product must be done under their terms. A machine readable copy of the corresponding portions of GPL licensed source code is available at the cost of distribution.

Such Open Source Software is distributed WITHOUT ANY WARRANTY, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. See the GPL and BSD for details.

A copy of the licenses is available from Lantronix. The GNU General Public License is available at http://www.gnu.org/licenses/.

Contacts

Lantronix Corporate Headquarters
15353 Barranca Parkway
Irvine, CA 92618, USA
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Online: www.lantronix.com/support

Sales Offices
For a current list of our domestic and international sales offices, go to the Lantronix web site at http://www.lantronix.com/about/contact/index.html

Disclaimer & Revisions

Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his or her own expense, will be required to take whatever measures may be required to correct the interference.

Note: *This equipment has been tested and found to comply with the limits for Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this User Guide, may clause interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user will be required to correct the interference at his or her own expense.*

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment.

Changes or modifications to this device not explicitly approved by Lantronix will void the user's authority to operate this device.

The information in this guide may change without notice. The manufacturer assumes no responsibility for any errors that may appear in this guide.

Date	Rev.	Comments
9/05	A	Initial Release
6/06	B	User Interface Enhancements: Improved usability (device/port search, improved UI, SecureLinx Detector for setup, updated webSSH applet, with increased scroll buffer, cut-and-paste capabilities, and font size adjustments). Simplified 'end-device only' view for users with a minimum of privileges. Expanded managed device (end-device) integration: Integration of SLK and SLP to the device port level. Device-type dependent processing and views.
7/06	C	Added capabilities: Enable, disable, and prioritization of local user authentication; additional (2) polled NTP servers; additional two (2) NIS slave servers; auto-detection of SCSxx00 devices; assignment of managed groups to selected ports, and automatic system backup increased up to 8 SLMs. Modifications to GUI and command line interfaces.
12/06	D	Added capabilities: IPv4 Filters; modem management; virtual managed devices for easier administration; uploading passwords in bulk; additional search options; get/put SSH keys; new triggers for events; device folder state management; session termination; discovery protocol using multicast.
4/07	E	Added capabilities: Access SLM by mobile phone; discover USB modems; view session log files; change SNMP settings for SLPs in bulk; connect directly to the port of an SLC or BOB; apply power to multiple ports on an SLP; view port logs, make a web channel connection to an SLC; update SLM and SLP firmware; read SLC information to the SLM database; create banners for the CLI.

Date	Rev.	Comments
11/07	F	Added capabilities: More Ethernet devices to manage (SLB, WiBox, UDS, Spider); IPsec Management (IKE Policies and VPN Connections); SecurID authentication; WiBox and UDS firmware updates; enhanced SLM update feature; port access for SLC, SLB, SLP and Spider); SLM proxy; additional trigger types for events; more file types to manage.

Table of Contents

Copyright & Trademark 2
Open Source Software 2
Contacts 2
Disclaimer & Revisions 3

1: About This Guide 15
Purpose and Audience 15
Chapter Summaries 15
Additional Documentation 17
Terminology 17

2: Introduction 20
Benefits 20
IT Management Application 21
Firmware 21
Protocols Supported 22
Hardware 22
Product Information Label 23
Package Contents 23

3: Quick Setup 24
Installing the SLM 24
Connecting a Terminal to the Console Port 24
Connecting to a Network Port 25
Connecting to the Power Supply 25
Monitoring the LEDs 25
Quick Network Setup 26
Required Information 26
Using Detector 26
Using Quick Setup on the Command Line Interface 29
Using the Web Interface 31
Quick Setup Command 35
Next Steps 35

4: Web and Command Line Interfaces 36
Web Interface 36
Logging in 36
Typical SLM Web Page 37
Notes 38
Web Page Help 39
Logging out 40
Command Line Interface (CLI) 40
Logging in 40
Commands 41
Command Help 42
Tips 42
Logging out 42
CLI Commands 43

Session Commands 43
5: Configuration and Operation Overview 45
Step 1: Configure Network Settings 45
Step 2: Define Authentication Methods 45
Step 3: Set Up User Account Groups and Accounts 46
Step 4: Auto-Detect Devices 46
Step 5: Associate Account Groups with Ethernet and Managed Devices 46
Step 6: Manage Devices 46
Step 7: Maintain the SLM 47
6: Network and Modem Settings 48
IP Address and Other Required Information 48
Using the Web Interface 49
Network Port(s) 49
Network Gateways 52
Viewing Network Statistics 53
Changing the Current User's Password 54
Network Commands 55
IPv4 Filters 56
Viewing a List of IPv4 Filters 56
Adding an IPv4 Filter 57
Updating or Deleting an IPv4 Filter 59
Viewing the System IPv4 Filter Sets 60
Setting Properties of an IPv4 Filter 60
IPv4 Filter Commands 62
IPsec Management 64
Internet Key Exchange (IKE) Policies 64
Viewing a List of IKE Policies 64
Adding an IKE Policy: 65
Updating or Deleting an IKE Policy 67
VPN Connections 68
Viewing a List of VPNs 68
Adding a VPN 69
Updating or Deleting a VPN 71
Connecting a VPN 71
Modem Management 72
Viewing a List of Modems 72
Configuring a Modem 73
Enabling or Disabling Dial-in Connections 74
Viewing a List of Connections 75
Adding a Connection 76
Updating and Deleting a Connection 78
Discovering a USB Modem 79
Modem Commands 80
Dial Account Commands 81
7: User Management 84

User Authentication Methods 84
NIS 87
LDAP 88
RADIUS 89
Kerberos 90
TACACS+ 92
SecurID 93
SSH Keys 94
Copy Keys 97
Authentication Commands 97
Account Groups 101
Account Group Types 101
Viewing Account Groups 101
Adding an Account Group 102
Updating or Deleting an Account Group 103
Setting Password Requirements for Account Groups 103
Assigning Account Group Device Rights 105
Viewing Currently Logged-In Accounts 107
Account Group Commands 108
Accounts 109
Viewing Accounts 109
Adding an Account to the Administrators Account Group 111
Adding an Account to an Ethernet or Managed Device Account Group 114
Updating or Deleting an Account 115
Account Commands 116
8: Ethernet Device Management 119
Auto-Detecting Devices 119
Auto-Detect Commands 122
Ethernet Devices 124
Listing Devices 124
Adding a Device Manually 125
Updating or Deleting Ethernet Device Settings 127
Polling 130
Viewing Session Log Files 131
Traps 132
Properties (Ethernet Device Menu Tree) 134
Port Access 135
Updating Passwords in Bulk 138
Changing SNMP Settings for SLPs in Bulk 139
SLM Proxy 139
Ethernet Device Commands 140
Trap Commands 143
Ports 145
Viewing a List of Ports 145
Adding a Port 146
Updating or Deleting a Port 149
Connecting Directly to the Port of an SLC or BOB 151

Statistics 151
Applying Power to SLP Ports on a Single Device 152
Viewing Port Logs 153
Port Commands 153
9: Managed Devices 156
Managed Device Groups 158
Viewing All Managed Devices 158
Viewing Managed Device Groups 159
Adding a Managed Device Group 160
Updating or Deleting a Managed Device Group 160
Configuring Polling Settings 161
Managed Device Group Commands 162
Connecting to a Managed Device 163
Creating Individual Managed Devices 164
From a Port 165
From a Ports List 166
From an Ethernet Device 167
Fusing Managed Devices 168
Methods of Fusing 168
Guidelines 168
Fusing a Port with an Existing Managed Device 168
Fusing an Ethernet Device with an Existing Managed Device 169
Continuing the One-at-a-Time Fusion Process 170
Fusing Managed Devices on the Managed Device Group Page 170
Configuring a Modem Connection to a Managed Device 172
Configuring a Managed Device 173
Updating or Deleting a Managed Device 174
Managed Device Commands 175
Administrators, Ethernet Account Users and Menu Only Users 175
Managed Device Users 177
10: Operation and Maintenance 179
Searching for Ethernet Devices, Ports, Managed Devices, and Users 179
Search for an Ethernet Device 179
Search for Ports 181
Search for Managed Devices 182
Search for Users 184
Using Wildcards 185
Search Commands 186
Connecting to Ethernet and Managed Devices 187
Connections Overview 187
Ethernet Devices – Connection Methods 188
Managed Devices – Connection Methods 188
Browsing to an Ethernet or Managed Device's Web Page 189
Making a Secure Channel Connection to an SLC, SLM, or SLB 189
Making an SSH Connection to an Ethernet or Managed Device 191
Making a Web Channel Connection to an SLC 192
Making a Telnet Connection to an Ethernet device 193

Connection Commands 194
Administrators, Ethernet Users and Menu Only Users 194
Managed Device Users 195
Services 196
Banners 197
SSL 198
Status 199
Services Commands 199
Maintenance 200
Maintenance Commands 203
Date and Time 205
Date and Time Commands 207
SNMP & Syslog 207
Device Firmware Updates 209
SLM Firmware 209
SLC Firmware 210
SLP Firmware 212
Spider Firmware 213
WiBox Firmware 214
UDS Firmware Updates 216
Managing Alternate SLMs 217
Managing SLCs 217
Using the Actions Tab 217
Rebooting or Shutting Down 219
Use the Actions tab to reboot or shut down one or more SLCs. 219
Getting a Log File 219
Getting or Restoring a Configuration File 219
Getting a Sysconfig File 220
Getting or Pushing SSH Keys 220
Reading Information 221
Issuing a CLI Command 221
Viewing Progress of Update FW and CLI Commands 222
Events 223
Event Management 223
Updating and Deleting Events 228
Viewing the Event Log 229
Clearing the Event Log 229
Files 230
File Types 230
File Format 231
Viewing, Deleting, and Renaming Files 231
Exporting, Uploading, and Downloading Files 233
Copying Files 234
Setting up NFS 235
Setting up CIFS 236
Setting up Log Properties 237
Logging Commands 239

11: Using SLM on a Mobile Browser 244
Requirements 244
Using the SLM Mobile Browser 244
Logging in to the SLM 244
Using Links to Select Options 245
Using the Keypad to Select Options 245
Obtaining More Data 246
Logging Out 246
Navigation Summary 247
Main Menu 247
Status Menu 248
System Information 248
Connections 248
Route Information 249
Device Menu 250
Ethernet Devices 250
Ethernet Unreachable Devices 252
Managed Devices 253
Log Menu 253
Filtering Logs 253
View Logs 254
A: Command Reference 257
Introduction to Commands 257
Command Syntax 257
Command Help 258
Tips 258
Authentication Commands 259
Account Commands 262
Account Group Commands 264
Administrative Commands 265
All Devices Commands 269
Auto-Detect Commands 269
CLI Commands 271
Connection Commands 272
Administrators, Ethernet Users and Menu Only Users 272
Managed Device Users 274
Date and Time Commands 275
Diagnostic Commands 275
Dial Account Commands 277
Ethernet Device Commands 279
IPv4 Filter Commands 283
Logging Commands 284
Audit Log 285
Event Log 286
Port Log 287
Session Log 289

System Log 290
Trap Log 291
Maintenance Commands 293
Managed Devices 295
Administrators, Ethernet Account Users and Menu Only Users 295
Managed Device Users 298
Menu Commands 299
Modem Commands 300
Network Commands 302
Port Commands 304
Search Commands 306
Services Commands 307
Session Commands 308
SSH Key Commands 309
Task Progress Command 310
B: Security Considerations 311
Security Practice 311
Factors Affecting Security 311
Available Services and Port Numbers 311
C: Safety Information 313
Safety Precautions 313
D: Technical Specifications 315
E: Compliance Information 316
SLM-01 316
SLM-02 317
F: Protocol Glossary 318
G: Warranty 321

Figures

Figure 1-1. Rights of Ethernet Device Group and Managed Device Group to Devices ------ 19
Figure 2-1. SLM Overview ------ 21
Figure 2-2. Front View of SLM ------ 22
Figure 2-3. Back View of SLM ------ 23
Figure 3-1. Connections ------ 24
Figure 3-2. LEDs on Front of SLM ------ 25
Figure 3-3. Lantronix Detector Window ------ 27
Figure 3-4. Detector Device List Window ------ 27
Figure 3-5. Network Settings Window ------ 28
Figure 3-6. Beginning of Quick Setup Script ------ 29
Figure 3-7. Completed Quick Setup ------ 30
Figure 3-8. SLM Home Page ------ 31
Figure 3-9. Network – Settings Page ------ 32
Figure 3-10. Network Settings – Statistics Tab ------ 33
Figure 3-11. Date & Time Page ------ 34
Figure 3-12. Account Page for sysadmin ------ 35
Figure 4-1. Web Page Layout ------ 37

Figure 4-2. Tree Structure on the Menu ---- 38
Figure 4-3. Note for an Account Group ---- 39
Figure 4-4. Example of a Help Page ---- 39
Figure 4-5. Logout on the Page Header ---- 40
Figure 4-6. Actions and Category Options ---- 41
Figure 6-1. SLM Configuration Page ---- 49
Figure 6-2. Network Settings Page ---- 50
Figure 6-3. Network Settings – Statistics Tab ---- 52
Figure 6-4. Network Settings – Statistics Tab ---- 54
Figure 6-5. Configuration Page – Password Tab ---- 54
Figure 6-6. IPv4 Filter Definitions – List Tab ---- 57
Figure 6-7. New IPv4 Filter Definition – Configure Tab ---- 57
Figure 6-8. IPv4 Filter – Configure Tab ---- 59
Figure 6-9. IPv4 Filter Definitions – Show Tab ---- 60
Figure 6-10. IPv4 Filter – Show Tab ---- 60
Figure 6-11. IPv4 Filter Definitions – Properties Tab ---- 61
Figure 6-12. Internet Key Exchange Policies Page ---- 64
Figure 6-13. New IPv4 Filter Definition Page ---- 65
Figure 6-14. Internet Key Exchange Policiy -- Configure Tab ---- 67
Figure 6-15. VPN Connections Page ---- 68
Figure 6-16. VPN Connection -- Configure Tab ---- 71
Figure 6-17. Modems Page ---- 72
Figure 6-18. Modem Page – Configure Tab ---- 73
Figure 6-19. Modem Page – Dial in Tab ---- 74
Figure 6-20. Modem Connections – List Tab ---- 75
Figure 6-21. New Connection—Configure Tab ---- 76
Figure 6-22. Connection Page — Configure Tab ---- 79
Figure 7-1. User Authentication Page – Configure Tab ---- 85
Figure 7-2. NIS Authentication Page – Configure Tab ---- 87
Figure 7-3. LDAP Authentication Page – Configure Tab ---- 88
Figure 7-4. RADIUS Authentication Page – Configure Tab ---- 89
Figure 7-5. Kerberos Authentication Page – Configure Tab ---- 91
Figure 7-6. TACACS+ Authentication Page – Configure Tab ---- 92
Figure 7-7. SecurID Authentication Page ---- 93
Figure 7-8. Manage SSH Keys – SLM Keys Tab ---- 94
Figure 7-9. Manage SSH Keys – SLC Keys Tab ---- 96
Figure 7-10. Manage SSH Keys – Copy Keys Tab ---- 97
Figure 7-11. Account Groups Page – Accounts Tab ---- 102
Figure 7-12. Account Groups Page – Members Tab ---- 102
Figure 7-13. Account Group Page – Group Tab ---- 102
Figure 7-14. Account Groups – Group Tab ---- 103
Figure 7-15. Account Groups Page – Passwords Tab. ---- 103
Figure 7-16. Ethernet Device Account Group – Accounts Tab ---- 105
Figure 7-17. Ethernet Device Account Group – Assign Tab ---- 105
Figure 7-18. Managed Device Account Group – Accounts Tab ---- 106
Figure 7-19. Managed Device Account Group – Assign Tab ---- 106
Figure 7-20. Account Groups – Connections Tab ---- 107
Figure 7-21. Account Groups -- Accounts Tab ---- 109
Figure 7-22. Account Page – Configure Tab ---- 111
Figure 7-23. Administrator Account Group – Accounts Tab ---- 111
Figure 7-24. Add New Account to Group – Configure Tab ---- 112
Figure 7-25. Add New Accounts to Group – Configure Tab ---- 114
Figure 7-26. Manage Account – Configure Tab ---- 116
Figure 8-1. Automatic Device Detection Page – Configure Tab ---- 119
Figure 8-2. All Ethernet Devices Page – List Tab ---- 124
Figure 8-3. Manage Group Page – List Tab ---- 125

Figure 8-4. Add SLM Device Page – Configure Tab ---------- 125
Figure 8-5. Add SLC Device Page – Configure Tab---------- 126
Figure 8-6. Add Spider Device Page – Configure Tab---------- 126
Figure 8-7. Add Other Lantronix Device Page – Configure Tab---------- 126
Figure 8-8. SLC Device Page – Configure Tab---------- 128
Figure 8-9. SLP Device Page – Configure Tab---------- 128
Figure 8-10. SLM Device Page – Configure Tab---------- 129
Figure 8-11. All Ethernet Devices -- Polling Tab ---------- 130
Figure 8-12. Device Page – Logs Tab ---------- 131
Figure 8-13. All Ethernet Devices Page -- Traps Tab---------- 133
Figure 8-14. All Ethernet Devices Page -- Properties Tab---------- 134
Figure 8-15. Manage SLC Group -- SLC Tab---------- 135
Figure 8-16. Mange SLB Group – Port Access Tab---------- 136
Figure 8-17. Manage SLP Group – Port Access Tab ---------- 136
Figure 8-18. Manage Spider Group – Port Access Tab ---------- 137
Figure 8-19. All Ethernet Devices Page – Passwords Tab ---------- 138
Figure 8-20.All Ethernet Devices Page – SNMP Tab ---------- 139
Figure 8-21. All Ethernet Devices – SLM Proxy Tab ---------- 140
Figure 8-22. Device -- Ports Tab ---------- 145
Figure 8-23. New SLC Port Page – Configure Tab---------- 147
Figure 8-24. Port Page – Configure Tab ---------- 150
Figure 8-25. Manage SLC Group Page – Port Access Page---------- 151
Figure 8-26. Connection to Selected SLC Port ---------- 151
Figure 8-27. Port Page -- Statistics Tab ---------- 152
Figure 8-28. SLP's Device Page -- Ports Tab---------- 152
Figure 8-29. Port Page – Logs Tab---------- 153
Figure 9-1. Virtual Managed Device---------- 157
Figure 9-2. Managed Device Groups Page – Devices Tab---------- 158
Figure 9-3. Managed Device Groups Page – List Tab---------- 159
Figure 9-4. Managed Device Group Page – List Tab ---------- 160
Figure 9-5. New Managed Device Group Page – Configure Tab ---------- 160
Figure 9-6. Managed Device Group Page – Configure Tab ---------- 161
Figure 9-7. Managed Device Groups – Polling Tab ---------- 161
Figure 9-8. Managed Device Page -- Connect Tab---------- 163
Figure 9-9. Port Page – Configure Tab---------- 165
Figure 9-10. Link to a Managed Device Page – Configure Tab ---------- 165
Figure 9-11. Managed Device Page – Connect Tab ---------- 166
Figure 9-12. Device Page - Ports Tab ---------- 166
Figure 9-13. Device Page for Cisco Switch---------- 167
Figure 9-14. Fusing on a Port Page – Configure Tab---------- 168
Figure 9-15. Virtual Managed Device Page with Two Connections ---------- 169
Figure 9-16. Fusing a Managed Device on the Device Page ---------- 169
Figure 9-17. Virtual Managed Device on Managed Device Page – Connect Tab---------- 170
Figure 9-18. Managed Device Group – List Tab ---------- 171
Figure 9-19. Managed Device Group Page – List Tab (After Fusion)---------- 171
Figure 9-20. Virtual Managed Device after Fusion---------- 172
Figure 9-21. Managed Device Page – Configure Tab---------- 172
Figure 9-22. Managed Device Page -- Modem Tab ---------- 172
Figure 9-23. Managed Device Page – Configure Tab---------- 173
Figure 9-24. Managed Device – Configure Tab ---------- 174
Figure 10-1. Search Fields---------- 179
Figure 10-2. Example of a Search by IP Address---------- 180
Figure 10-3. Example of a Search by Port---------- 182
Figure 10-4. Example of a Search by Managed Device---------- 183
Figure 10-5. Example of a Search by User---------- 185
Figure 10-6. Secure Channel Connection to an SLC ---------- 190

Figure 10-7. SSH Login to SLC ---------- 192
Figure 10-8. Web Channel Connection to an SLC ---------- 192
Figure 10-9. Telnet Connection ---------- 193
Figure 10-10. SLM Services Page ---------- 196
Figure 10-11. Services Page – Banners Tab ---------- 197
Figure 10-12. Services – SSLTab ---------- 198
Figure 10-13. Services Page – Status Tab ---------- 199
Figure 10-14. SLM Maintenance Page ---------- 201
Figure 10-15. Date & Time Page ---------- 205
Figure 10-16. SNMP& Syslog Page ---------- 207
Figure 10-17. Device Firmware Update Page – SLM Tab ---------- 209
Figure 10-18. Device Firmware Update Page -- SLC Tab ---------- 210
Figure 10-19. Device Firmware Update – SLP Tab ---------- 212
Figure 10-20. Device Firmware Update Page – Spider Tab ---------- 214
Figure 10-21. Device Firmware Update Page – WiBox Tab ---------- 215
Figure 10-22. Firmware Update Page – UDS Tab ---------- 216
Figure 10-23. Auto Saving a Configuration ---------- 217
Figure 10-24. Manage "SLC" Group Actions Tab ---------- 218
Figure 10-25. Issuing a CLI Command ---------- 222
Figure 10-26. Background Task Progress Page – Progress Tab ---------- 222
Figure 10-27. Background Task Progress – Dev Status Tab ---------- 223
Figure 10-28. Event Management Page – Events Tab ---------- 224
Figure 10-29. SNMP Trap Configuration (Lantronix Tech Support FAQ) ---------- 227
Figure 10-30. Manage Event Page –Event Tab ---------- 228
Figure 10-31. Event Management Page – Log Tab ---------- 229
Figure 10-32. SLM Syslog Files Page – Files Tab ---------- 232
Figure 10-33. SLM Syslog Files Page – Display Tab ---------- 232
Figure 10-34. Files Page ---------- 233
Figure 10-35. File Management Page – Copy Tab ---------- 234
Figure 10-36. File Management Page – NFS Tab ---------- 235
Figure 10-37. File Management – CIFS Tab ---------- 236
Figure 10-38. File Management Page -- Logging Tab ---------- 238
Figure 11-1. Actions and Category Options ---------- 258

1: About This Guide

Purpose and Audience

This guide provides the information needed to install, configure, and use the Lantronix SecureLinx™ Management Appliance (SLM). The SLM enables IT professionals to remotely and securely configure and administer multiple SecureLinx management devices.

Chapter Summaries

The remaining chapters in this guide include:

Chapter	Description
2: Introduction	Describes the SLM's main features and the protocols it supports.
3: Quick Setup	Provides instructions for getting your unit up and running. Describes connection formats and power supplies and how to configure network, date, and time settings so you can use the SLM on the network.
4: Web and Command Line Interfaces	Describes the web and command line interfaces available for configuring the unit. ***Note:*** *The configuration chapters (6-9) provide detailed instructions for using the web interface and include command line interface commands.*
5: Configuration and Operation Overview	Outlines the process of setting up and using the SLM and explains the responsibilities of administrators and other user groups.
6: Network and Modem Settings	Provides instructions on entering network, date, and time information.

Chapter	Description
7: User Management	Provides instructions for configuring user authentication methods and setting up user accounts and account groups.
8: Ethernet Device Management	Provides instructions for detecting devices on the network, entering information about the devices and ports, granting read/write permissions for devices and ports, and auto-saving an SLM configuration to another SLM.
9: Managed Devices	Explains how to add, update, and delete Managed Device Groups as well as how to create and "fuse" individual managed devices. Provides information about connecting to and configuring managed devices via the SLM.
10: Operation and Maintenance	Explains how the user can search for devices, access notes and logs about the SLC and its ports, and open the SLC, SLP, SLK and SLC interfaces using SSH, secure channel (SLC only), or a browser. Provides instructions for upgrading firmware, viewing system logs and diagnostics, and generating reports. Includes information about web pages and commands used to shut down and reboot the SLM.
11: Using SLM on a Mobile Browser	Provides instructions for accessing and monitoring the SLM using a mobile phone.
A: Command Reference	Lists and describes all of the commands used on the SLM command line interface.
B: Security Considerations	Provides tips for enhancing SLM security.
C: Safety Precautions	Lists safety precautions for using the SLM.
D: Technical Specifications	Lists information about the SLM hardware.
E: Compliance Information	Provides information about the SLM's compliance with industry standards.
F: Protocol Glossary	Briefly describes networking protocols.

Additional Documentation

The following information is available on the product CD, the Lantronix web site (www.lantronix.com), or the product itself:

Document	Description
SLM Quick Start	Describes the steps for getting the SLM up and running; provided in printed form.
SLM Online Help for the Command Line Interface	Provides online Help for configuring and operating the SLM using commands.
SLM Online Help for the Web Interface	Provides online Help for configuring and operating the SLM using the web interface.
Detector Online Help	Provides online Help for the utility that enables you to change an automatically assigned IP address to a static IP address quickly.

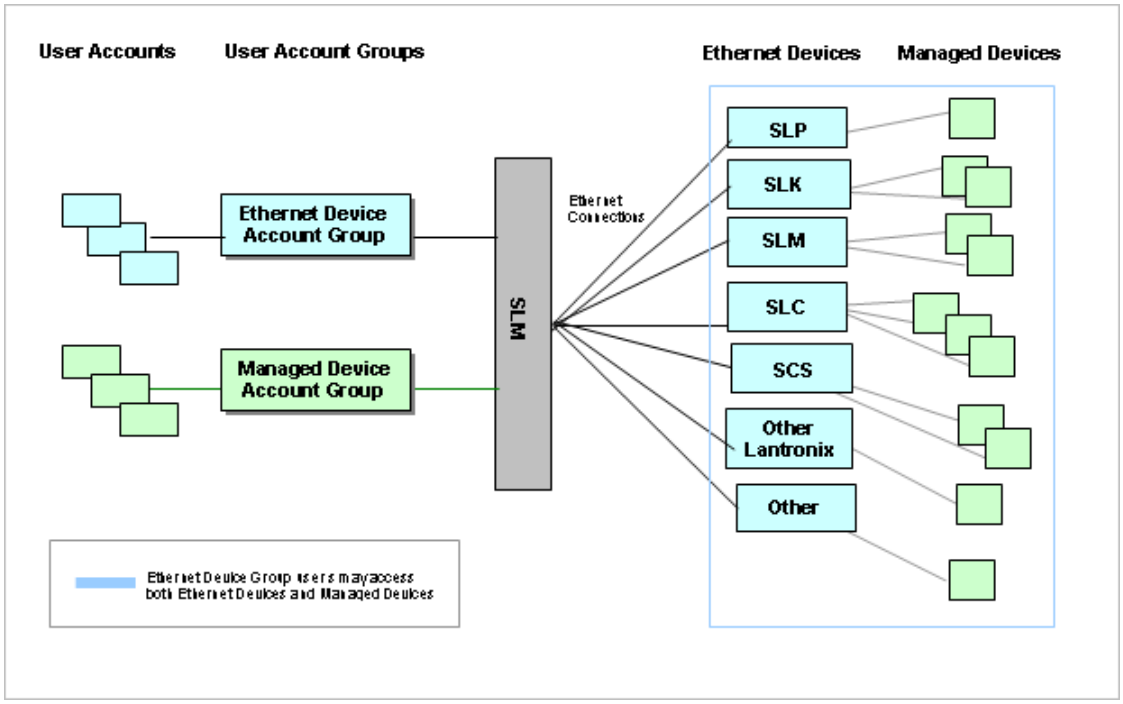
Terminology

In this User Guide, we use the following terms:

Term	Definition
Ethernet Device	A Lantronix or non-Lantronix device that the SLM discovers on the network. Ethernet devices include: **SecureLinx Management Devices:** Members of the Lantronix SecureLinx IT Management family of products: the SecureLinx Console Manager (SLC), SecureLinx Remote Power Manager (SLP), SecureLinx Remote KVM Manager (SLK), WiBox, Branch Office Box (BOB),and Spider. These devices enable you to remotely and securely access and manage networking equipment. **Management Devices:** Lantronix devices that enable you to manage networking equipment. The SCS05/20 is an example. **Lantronix Devices:** Other Lantronix products that network-enable serial devices so you can remotely control, monitor, diagnose, and troubleshoot your equipment over a network or the Internet. **Other Devices:** Non-Lantronix Ethernet devices.
Port	A connector (e.g., serial, power, or KVM) on a management device (e.g., SLC, SLP, SLK, SCS) that allows for control of another device.

Term	Definition
Managed Device	A device (such as a Unix server) that has one or more of its connections (e.g., serial, power, or KVM) exposed to allow control and configuration changes by Managed Device Users. A managed device belongs to a Managed Device Group.
Managed Device Group	A group created to allow logical clustering of managed devices (e.g., devices of the same type or devices in the same physical location). A managed device may not be created until at least one Managed Device Group has been defined.
Account	Individual users; must belong to an account group, from which they inherit permissions.
Account Group	A group of accounts (users) with the same privileges. The four types of account groups include: **Administrators Group:** The sysadmin account, which has all privileges and others with specified configuration privileges. ***Note:*** *Throughout this user guide, the term "administrator" means the person using the* ***sysadmin*** *user name and those members of the Administrators Group permitted to perform the task.* **Ethernet Device Account Groups:** Have access to specified Ethernet devices and the managed devices connected to them. **Managed Device Account Groups:** Have access to devices attached to specified Ethernet device ports. **Menu Only Account Groups:** May only access the command line interface and use a limited menu of options.

Figure 1-1. Rights of Ethernet Device Group and Managed Device Group to Devices



2: Introduction

The SecureLinx Management Appliance (SLM) is a member of the Lantronix SecureLinx IT Management family of products, which includes the SecureLinx Console Manager (SLC), SecureLinx Remote Power Manager (SLP), and SecureLinx Remote KVM (SLK). These products offer systems administrators and other IT professionals a variety of tools for remotely and securely accessing and managing their networking equipment. You can even access the system using a cell phone.

Note: For more information about the product family, see the Lantronix web site at http://www.lantronix.com

The SLM manages SecureLinx management devices. It "auto-detects" and then displays them in a single, concise view through a web or a command line interface (CLI). A user can search the web view for a desired device or device port (in the case of an SLC or SLK) and then connect to a found device or port without using a separate interface. With an SLC, the user logs in only once, to the SLM, and then any subsequent device logins are automatic. The SLM can also use LDAP, RADIUS, NIS, Kerberos, TACACS+, and SSH public key to authenticate users connecting remotely to the command line interface.

Note: *The SLM is designed to work in an exclusively Lantronix environment. In a mixed environment, the necessary protocols may not be available to provide the same level of functionality.*

Benefits

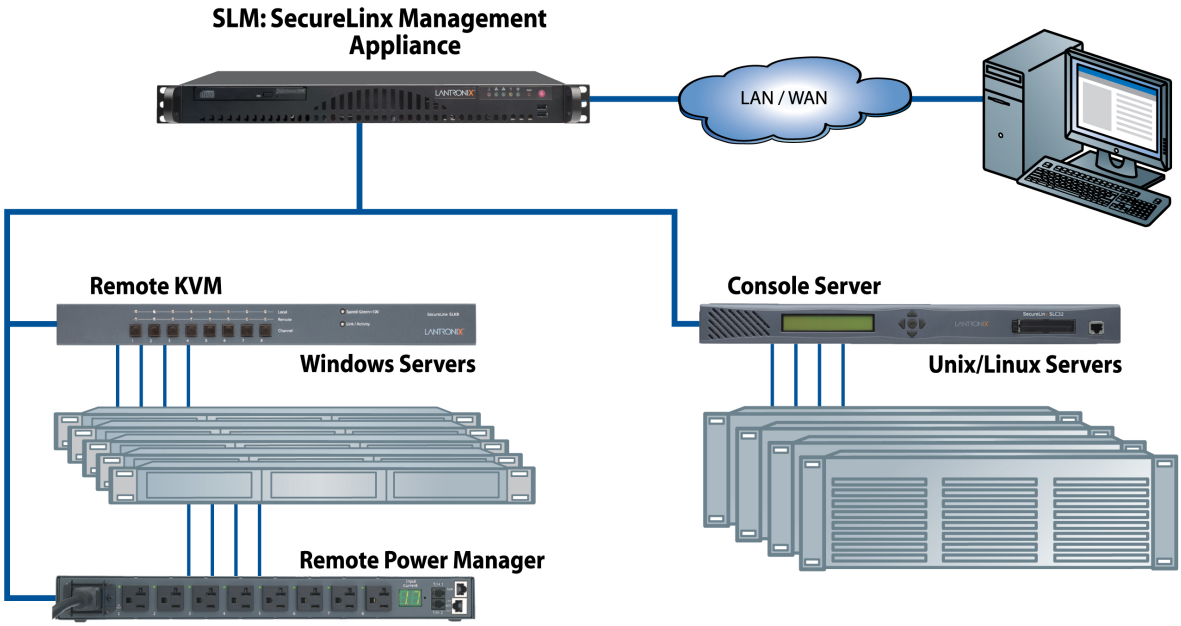
With the SLM, you can:

- Consolidate management of IT infrastructure through a simple browser interface.
- Maintain a secure, central point of access to all equipment with centralized console logging.
- Reduce equipment diagnosis and repair time while minimizing the cost of ownership and administrative resources.
- Maintain more network up time.

IT Management Application

The following diagram shows how a user can perform SecureLinx management activities through the SLM.

Figure 2-1. SLM Overview



Firmware

The SLM firmware has the following features:

- Access to up to 256 devices
- User and events logging
- Email notification of trap events, log file events, and Ethernet down
- ID/Password security, configurable access rights
- SSH and SSL security
- External authentication through RADIUS, LDAP, NIS, Kerberos, and TACACS+
- Shared authentication among SLMs and SLCs
- SLC firmware version storage and updates
- Local access through a console port
- Web presentation of SLC and ports in a user-configured view
- Web administration (using most browsers)
- Direct SSH access to SLCs or SLC ports from the web view
- Auto-discovery of SecureLinx management devices and other Lantronix and non-Lantronix Ethernet devices

- Support for an internal PCI or external USB modem
- SNMP MIB2
- SNMP trap target
- Mobile phone WAP browser access

Protocols Supported

In addition to supporting the TCP/IP network protocol, the SLM supports:

- SSH for connections in and out of the SLM
- SMTP for mail transfer
- SNMP for remote monitoring and management
- SFTP and FTP for file transfers and firmware upgrades
- DHCP and BOOTP for IP address assignment
- HTTPS (SSL) for secure browser-based configuration
- NTP for time synchronization
- LDAP, NIS, RADIUS, Kerberos, and TACACS+, SecurID, and SSH public key encryption for remote user authentication
- WAP for mobile phone access

For brief descriptions of these protocols, see *F: Protocol Glossary*.

Hardware

The SLM-01 and SLM-02 hardware has the following features:

- 1U rack mountable
- Two network ports for conventional Ethernet network; uses standard RJ45-terminated Category 5 cables:
  - SLM-01: One 10/100Base-T and one 10/100/1000Base-T connection
  - SLM-02: Two 10/100/1000Base-T connections
- DB9 RS-232 serial console port for VT100 terminal or PC with emulation
- AC input voltage of 100 to 240 VAC with 50 or 60 Hz
- Operating temperature range of 50°F to 95°F
- PCI expansion slot
- DB25F parallel port (currently disabled) (SLM-02 only)
- USB ports: SLM-01 has three; SLM-02 has four

Note: *For more detailed information, see D: Technical Specifications.*

Figure 2-2. Front View of SLM

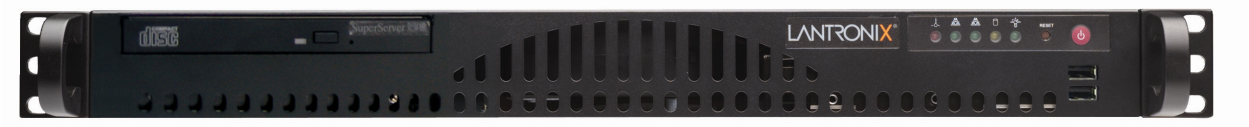
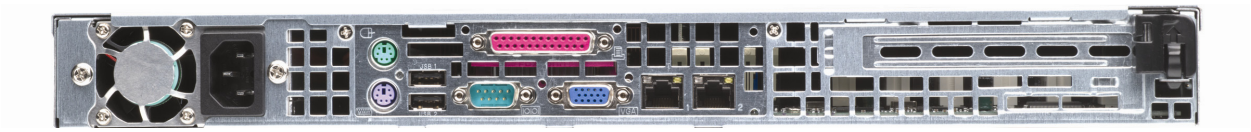


Figure 2-3. Back View of SLM



Product Information Label

The product information label on the underside of the unit contains the following information about each specific unit:

- Part Number
- Serial Number Bar Code
- Serial Number and Date Code
- Regulatory Certifications and Statements

Package Contents

In addition to the SLM, the box contains the following items:

- Quick Start Guide
- Null modem DB9 serial cable
- Power cord
- Rack slide kit
- Product CD containing Detector (utility for assigning an IP address), .Net Framework, the SecureLinx Management Device (SLM) User Guide and Command Reference. Verify and inspect the contents of the SLM package using the enclosed packing slip or the list above. If any item is missing or damaged, contact your place of purchase immediately.

3: Quick Setup

This chapter provides instructions for installing the SLM, getting it up and running, and entering basic network settings so you can configure and use the SLM on a network.

Caution: ***To avoid physical and electrical hazards, please be sure to read B: Safety Information before installing the SLM.***

Installing the SLM

Installation includes setting the SLM up in a rack and making serial console port (for initial setup only), network, and power connections.

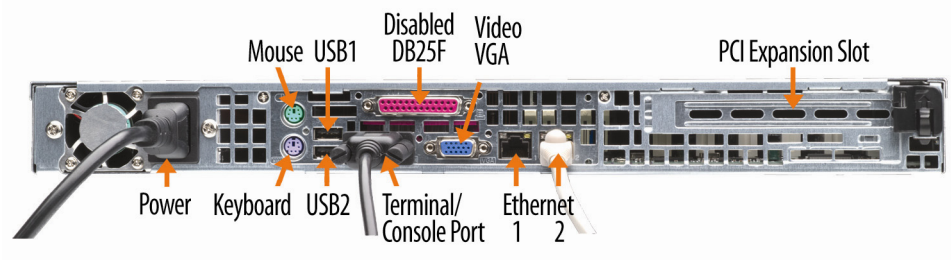
To install the SLM:

1. Place the unit in a 19-inch rack.

   Warning: ***Be careful not to block the air vents on the front and back of the unit. If you mount the SLM in an enclosed rack, we recommend that the rack have a ventilation fan to provide adequate airflow through the unit.***

2. For initial configuration, connect a terminal or a computer with terminal emulation to the console port. See *Connecting a Terminal to the Console Port* on page 24.
3. Connect the power cord and apply power. See *Connecting to the Power Supply* on page 25.
4. Wait approximately a minute and a half for the boot process to complete.

Figure 3-1. Connections



Note: *The PS/2 and VGA connectors are not used.*

Connecting a Terminal to the Console Port

The serial console port is for local access to the SLM. You can attach a dumb terminal or a computer with terminal emulation to the console port using a null-modem serial cable with DB9 on the SLM side. The SLM console port uses RS-232C protocol and supports VT100 emulation. The console port is configured as DTE. The default baud rate is 9600.

Connecting to a Network Port

The SLM's two network ports allow remote access to SLCs, SLKs, and SLPs and their attached devices and to system administrative functions. Use a standard RJ45-terminated Category 5 cable to connect to a network port).

Notes:

- *SLM-01 has one 10/100Base-T and one 10/100/1000Base-T network port; SLM-02 has two 10/100/1000Base-T network ports.*
- *One possible use for the two Ethernet ports is to have one port on a private, secure network, and the other on an unsecured network.*
- *Both Ethernet ports should not be on the same subnet.*

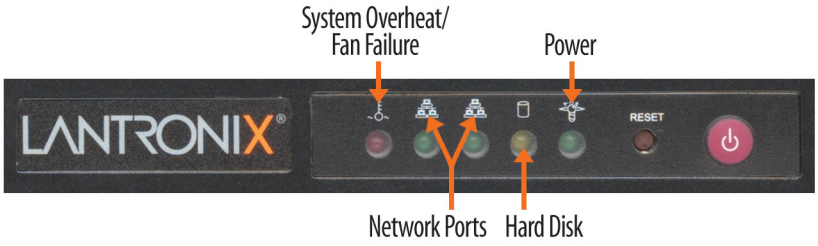
Connecting to the Power Supply

The SLM has a universal auto-switching AC power supply. The power supply accepts AC input voltage between 100 and 240 VAC with a frequency of 40 or 60 Hz. A rear-mounted IEC-type AC power connector provides universal AC power input (North American cord provided).

Monitoring the LEDs

The SLM has five LEDs on the front panel to signal information during boot-up and while the SLM is running.

Figure 3-2. LEDs on Front of SLM



SLM LED Functions

LED	Function
Power	Steady green when power is on.
Hard drive	Blinking yellow when there is hard drive access (typical PC LED).
Network Port 1	Green indicates activity.
Network Port 2	Green indicates activity.
System Overheat/Fan Failure	Steady yellow if the unit overheats. ***Warning:*** *If the alarm LED is on, quickly shut down the SLM and contact Lantronix Tech Support at* ***www.lantronix.com/support****. Continued use of the SLM while the alarm indicator is on may cause permanent system damage to hardware and data stored in the system.*

Quick Network Setup

This section helps get the IP network port up and running quickly, so you can administer the SLM using your network. Your SLM must have a unique IP address on your network. The SLM receives an IP address in one of three ways:

Automatically: The first time you power up the SLM, Network Port 1 tries to obtain its IP address via DHCP. If you have connected Network Port 1 to a network with a DHCP server, it acquires an IP address. Smaller networks may use BOOTP.

Using Detector: This software, included on the product CD, allows you to quickly assign a static IP address to a unit that has an automatically assigned IP address.

Manually: If the SLM cannot obtain an IP address by means of DHCP, you must manually enter one using a terminal or a PC running a terminal emulation program to the unit's serial console port.

The administrator generally provides the IP address and corresponding subnet mask and gateway. If you assign an IP address manually, **it must be within a valid range and unique to your network**.

Required Information

To set up the SLM quickly so you can use it on your network, you must first enter some basic information about one network port and the network.

IP address (if not already assigned): _____. _____ . _____ . _____

Subnet mask (if not already assigned): _____. _____ . _____ . _____

Gateway: _____. _____ . _____ . _____

Using Detector

The Detector software is on the product CD. Use Detector to replace an automatically assigned IP address with a static IP address.

> ***Note:*** *If you try to run **detector2.exe** on a network shared drive, you may get a security exception. We recommend that you run the program on the CD or copy the detector2 directory to your local hard drive and run it from there. If you must run **detector2.exe** from a network shared drive, you need to change your security settings using the" .NET Framework Configuration" or "caspol" tool.*

To install Detector:

1. Double-click **detector2.exe** on the product CD.
2. If a "The application failed to initialize properly (0xc0000135), click **OK** to terminate the application" message displays, you need to install .NET Framework.

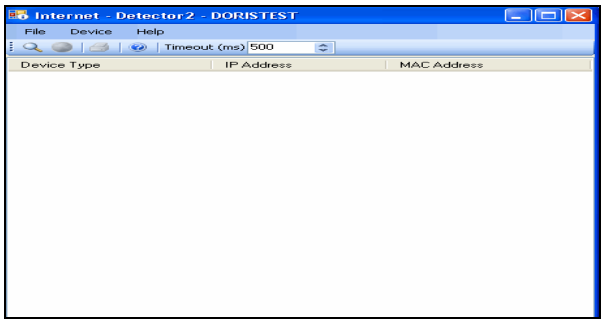
   Obtain the .NET Framework redistributable package from the SLM CD. It is also available as a stand-alone executable file, **Dotnetfx.exe**. You can download this from Microsoft at:

   http://www.microsoft.com/downloads/details.aspx?FamilyID=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=en

To use Detector to set the IP address:

1. Open the Detector software. The Lantronix Detector window opens.

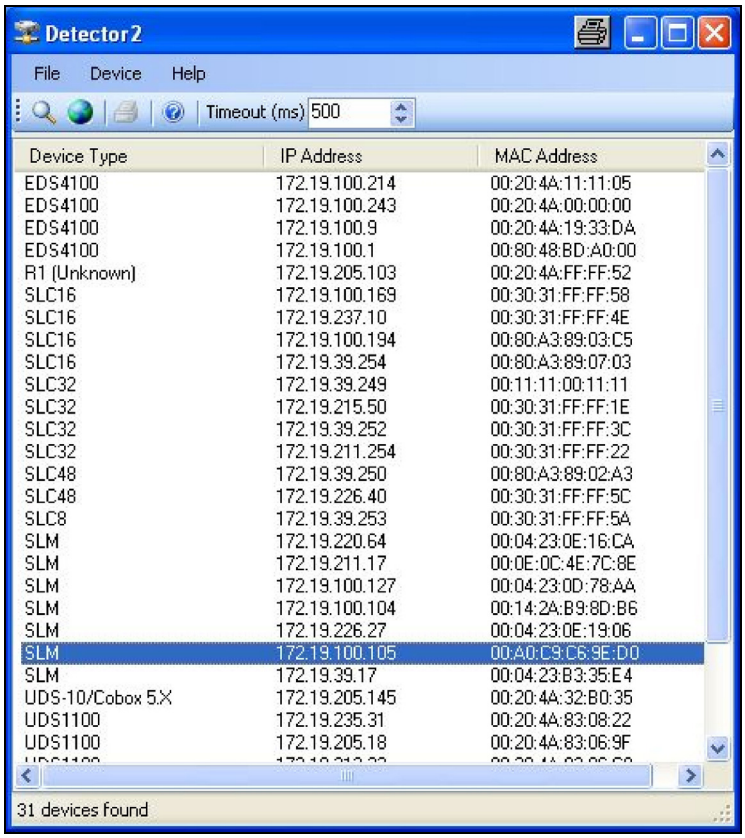
Figure 3-3. Lantronix Detector Window



2. From the **Timeout** drop-down menu (in the toolbar), select the number of milliseconds before the search stops. The default is **500**.

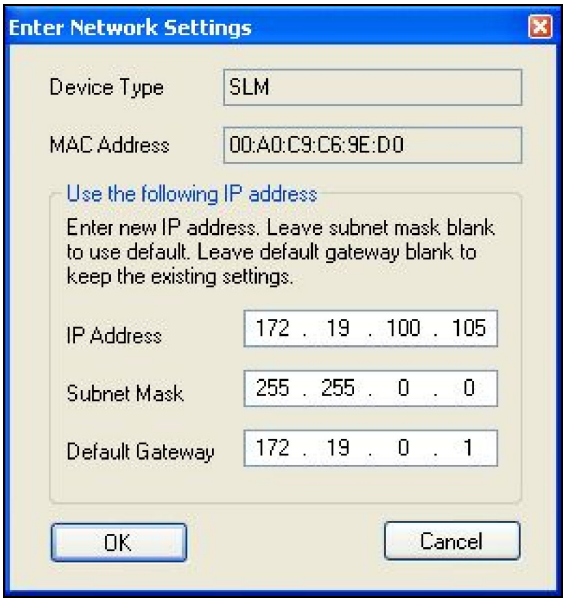
3. Click the **Search** icon . A list of Lantronix Ethernet devices on the network displays.

Figure 3-4. Detector Device List Window



4. If the SLM has an automatically assigned IP address and you want to change it, select the SLM and click the **Network Settings** icon . The Enter Network Settings window displays.

Figure 3-5. Network Settings Window


Enter Network Settings
Device Type
SLM
MAC Address
00:A0:C9:C6:9E:D0
Use the following IP address
Enter new IP address. Leave subnet mask blank to use default. Leave default gateway blank to keep the existing settings.
IP Address
172 . 19 . 100 . 105
Subnet Mask
255 . 255 . 0 . 0
Default Gateway
172 . 19 . 0 . 1
OK
Cancel

The **Device Type** and **MAC Address** (Ethernet Address) fields identify the unit.

5. Enter the following information:

IP Address	An IP address that will be unique and valid on your network and in the same subnet as your PC. There is no default. ***Note:*** *Enter all IP addresses in dot quad notation.*
Subnet Mask	The subnet mask specifies the network segment on which the SLC resides. To accept the default, leave blank.
Default Gateway	IP address of the router for this network. To accept the default, leave blank.

6. Click **OK**. A message confirms that your network configuration has been sent.
7. Click **OK**.
8. To confirm the change, click the **Search icon** and verify that the unit has new network settings.

Note: *IP address reassignment is only effective if the CLI quick setup or web network setting has not been configured before. Once you change the IP address using Detector, the network setting recognizes it as the static IP. You must set up a default gateway prior to using the Lantronix Discovery Protocol (LDP) to discover devices that support LDP, such as SLC devices. (See* *Auto-Detecting Devices on page 119.**)*

Using Quick Setup on the Command Line Interface

If the SLM does not have an IP address, connect a dumb terminal or a PC running a terminal emulation program (VT100) to access the command line interface. If the unit already has an IP address, you can use SSH to connect to the command line interface and add or change the IP address or other network-related information.

To complete the command line interface Quick Setup script:

Note: *4: Web and Command Line Interfaces describes the command line interface in detail.*

1. Do one of the following:
   - With a serial terminal connection, power up, and when the command line displays, press **Enter**.
   - With a network connection, use an SSH program to connect to **xx.xx.xx.xx** (the IP address in dot quad notation) and press **Enter**. The **login** prompt displays.
2. Type **sysadmin** (case sensitive) as the user name and press **Enter**.
3. Type **PASS** (case sensitive) as the password and press **Enter**.

Figure 3-6. Beginning of Quick Setup Script

```
Welcome to the SecureLinx Manager
Version: 3.2
Login Name: sysadmin
Login Time: Wed July 25 15:24:35 2007
For a list of commands, type 'help'.
Do you want to do quick setup? [no]
```

4. In response to the prompt asking whether you want to do the quick setup, type **yes** and press **Enter.**

   Note: *The prompt displays the first time you log in only. If you want to run the script again, type* ***admin quicksetup****.*

5. Enter the following information at the prompts:

   Note: *To accept a default or to skip an entry that is not required, press* ***Enter****.*

Configure Port 1 or 2	Select one of the following: **<1> obtain IP Address from DHCP:** The unit will acquire the IP address and gateway from the DHCP server. (The DHCP server may provide the gateway, depending on its setup.) This is the default setting. **<2> obtain IP Address from BOOTP:** Permits a network node to request configuration information from a BOOTP "server" node. **<3> static IP Address:** Requires you to assign a static IP address manually. The administrator generally provides the IP address. ***Note:*** *For SLM-01, Network Port 1 is 10/100/1000Base-T, while Network Port 2 is 10/100Base-T. For SLM-02, both Network Ports 1 and 2 are 10/100/1000Base-T.*

IP Address (if specifying)	An IP address that will be unique and valid on your network and in the same subnet as your PC. There is no default. If you selected **DHCP** or **BOOTP**, this prompt does not display. ***Note:*** *Enter all IP addresses in dot quad notation.*
Subnet Mask	The subnet mask specifies the network segment on which the SLC resides. There is no default. If you selected **DHCP** or **BOOTP**, this prompt does not display.
Gateway IP Address	IP address of the router for this network.
Hostname	The default host name is **SLM**. The host name can be a short host name or a fully qualified domain name. For example, we might add lantronix.com to the factory default name of SLM to get SLM.lantronix.com. There is a 64-character limit (contiguous characters).
Time Zone	If the time zone displayed is incorrect, enter the correct time zone and press **Enter**. If the entry is not a valid time zone, the system guides you through selecting a time zone. A list of valid regions and countries displays. At the prompts, enter the correct region and country.
Date/Time	If the date and time displayed are correct, type **n** and continue. If the date and time are incorrect, type **y** and enter the correct date and time in the formats shown at the prompts.
Sysadmin password	Enter a new password for the **sysadmin** account. It can be up to 128 characters and is case sensitive.

Figure 3-7. Completed Quick Setup

```
Quick Setup will now step you through configuring a few basic settings.

The current settings are shown in brackets ('[]').
You can accept the current setting for each question by pressing <return>.

____Ethernet Port and Default Gateway_____________________________________________
The SLM has two ethernet ports, Port 1 and Port 2.
Current settings are:
Port State    IP address    Subnet mask Mode           IPv4 filter
---- -------- ------------- ----------- -------------- -----------
1    Static   172.19.220.64 255.255.0.0 Auto-negotiate (None)
2    Disabled 0.0.0.0       0.0.0.0     Auto-negotiate (None)
Configure Port 1 or 2: [1]
Configure Port 1:  (1) obtain IP Address from DHCP
                   (2) obtain IP Address from BOOTP
                   (3) static IP Address(172.19.220.64)
Enter 1-3: [3]
Enter IP Address: [172.19.220.64]
Enter Subnet Mask: [255.255.0.0]
Enter gateway IP Address: [172.19.0.1]
Specify a hostname: [DaveSLM]

____Time Zone_____________________________________________________________________
The current time zone is 'US/Pacific'.
Enter time zone: [US/Pacific]

____Date/Time_____________________________________________________________________
The current time is Thu Jul 26 15:05:35 2007
Change the current time? [n]

____Sysadmin Password_____________________________________________________________
New password: [<current password>]
Network settings will be updated, the current terminal may not work.
Please re-connect to SLM with new settings as needed.
[sysadmin@DaveSLM]>
```

Once you complete the Quick Setup script, the changes take effect immediately.

Using the Web Interface

Note: *4: Web and Command Line Interfaces* describes the web interface in detail.

Once the SLM has an IP address, you can use the web interface to configure required network parameters that determine how the SLM interacts with the attached network. The unit might have a DHCP-assigned IP address or one assigned manually using Detector or a serial connection to the command line interface.

To log in to the web interface:

1. Open a web browser (Netscape Navigator 6.x and later, Internet Explorer 6.0. and later, or Firefox 1.5, with JavaScript enabled).
2. In the URL field, type **https://** followed by the IP address of your SLM.
3. Log in using **sysadmin** as the user name and **PASS** as the password. The SLM Configuration page opens.

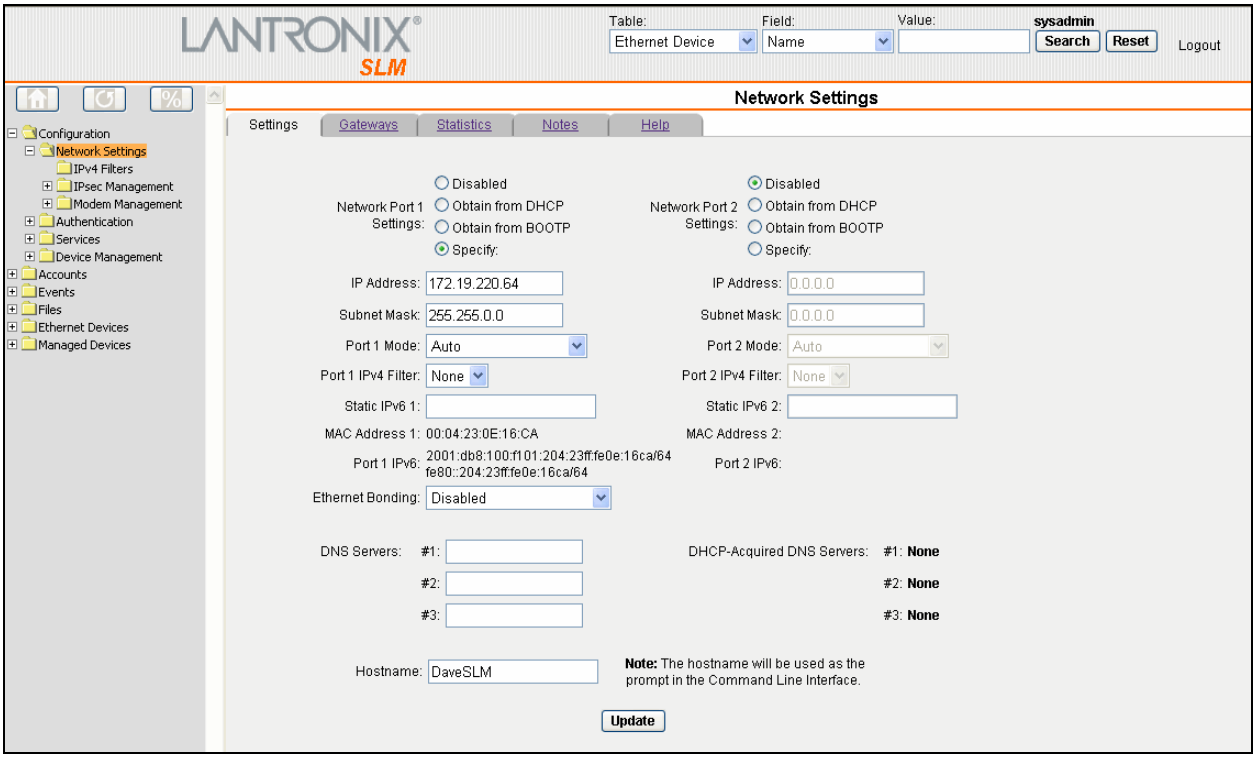
Figure 3-8. SLM Home Page

To enter settings for one network port:

Note: *For SLM-01, Network Port 1 is 10/100/1000Base-T, while Network Port 2 is 10/100Base-T. For SLM-02, both Network Ports 1 and 2 are 10/100/1000Base-T.*

1. On the menu (in the pane on the left), click **Configuration→ Network Settings**. The following page opens:

Figure 3-9. Network – Settings Page



2. Enter the following information for one network port:

Network Port 1

Network Port Settings	**Disabled:** This is the default setting for Network Port 2. **Obtain from DHCP:** Acquires IP address, subnet mask, and gateway from the DHCP server. (The DHCP server may provide the gateway, depending on its setup.) This is the default setting for Network Port 1. If you select this option, skip to step 3. **Obtain from BOOTP:** Lets a network node request configuration information from a BOOTP "server" node. Skip to step 3. **Specify**: Requires you to assign a static IP address manually. The administrator generally provides the IP address.
IP Address	If specifying an IP address, enter an IP address that will be within a valid range, unique to your network, and in the same subnet mask as your workstation. There is no default. ***Note:** Enter all IP addresses in dot quad notation.*
Subnet Mask	If specifying an IP address, enter the network segment on which the SLM resides. There is no default.

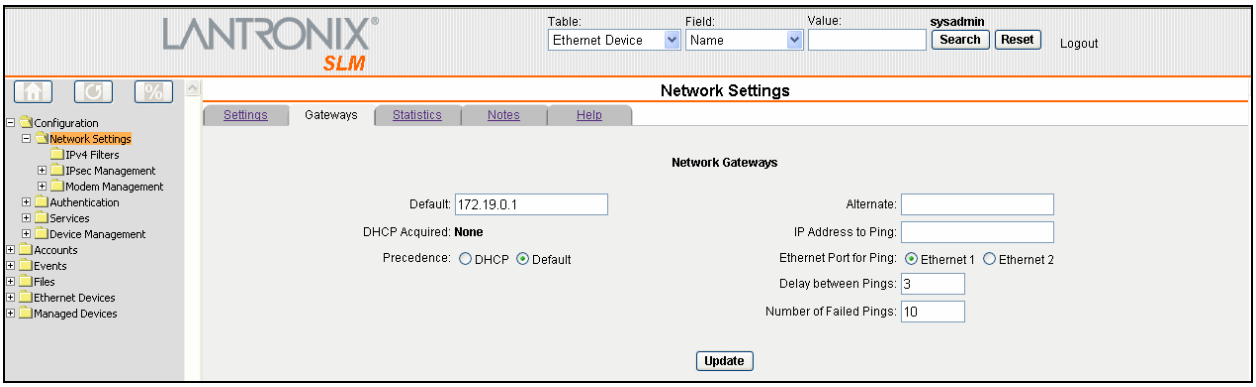
3. To save your entries, click **Apply**. Clicking **Apply** commits these changes immediately.

Next, enter network gateway information.

To enter gateway information:

1. On the Network – Settings page, click the **Gateways** tab. The following page opens:

Figure 3-10. Network Settings – Statistics Tab



2. Enter the following:

Default	IP address of the router for this network. If this has not been set manually, any gateway assigned by DHCP for Network Port 1 or Network Port 2 displays. All network traffic that matches the Network Port 1 IP address and subnet mask goes out Network Port 1. All network traffic that matches the Network Port 2 IP address and subnet mask goes out Network Port 2. If you set a default gateway, the SLM sends any network traffic that does not match Network Port 1 or Network Port 2 to the default gateway for routing.
DHCP Acquired (view only)	Gateway assigned by DHCP for Network Port 1 or Network Port 2. The default setting is **None**.
Precedence	Indicates whether the gateway assigned by DHCP or the default gateway takes precedence. The default setting is **DHCP Gateway**. If you select **DHCP Gateway**, and both network ports are configured for DHCP, the SLM gives precedence to the Network Port 1 gateway.

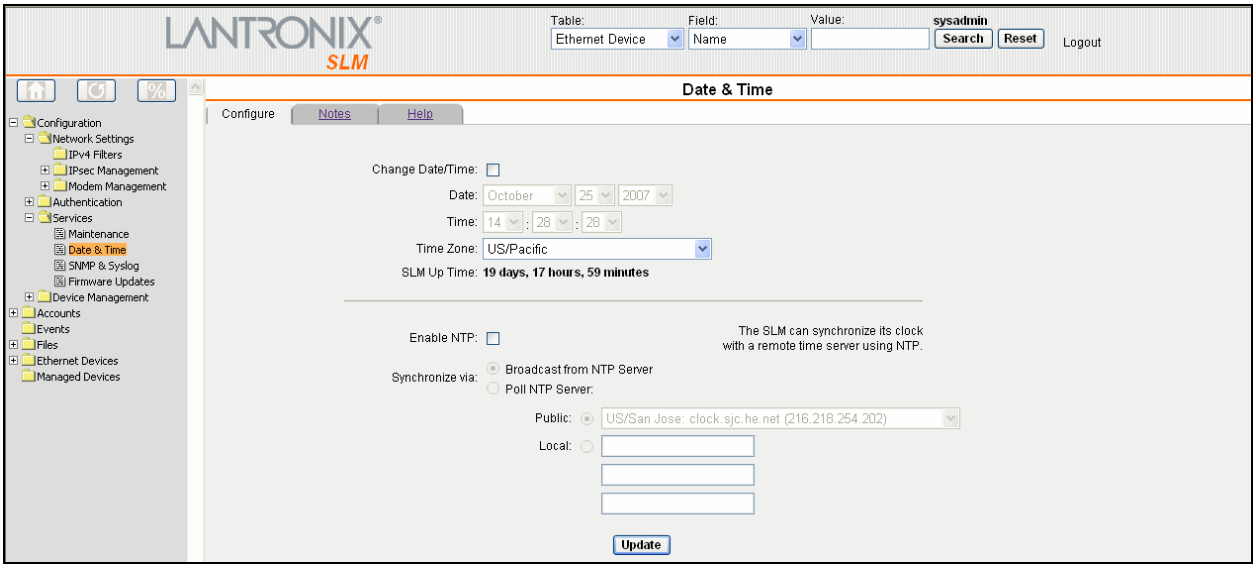
Note: *You have configured only the settings required to get the SLM up and running. To complete the network configuration, see* *6: Network and Modem Settings.*

To set the local date, time, and time zone:

You can specify the current date, time, and time zone at the SLM's location (default), or the SLM can use NTP to synchronize with an NTP server on your network.

1. On the menu, click **Configuration→Services→Date & Time**. The following page opens:

Figure 3-11. Date & Time Page



2. Enter the following information:

Date and Time

Change Date/Time	Select the check box to manually enter the date and time at the SLM's location.
Date	From the drop-down lists, select the current month, day, and year.
Time	From the drop-down lists, select the current hour and minute.
Time Zone	From the drop-down list, select the appropriate time zone.
SLM Up Time	Indicates how long the SLM has been up and running.

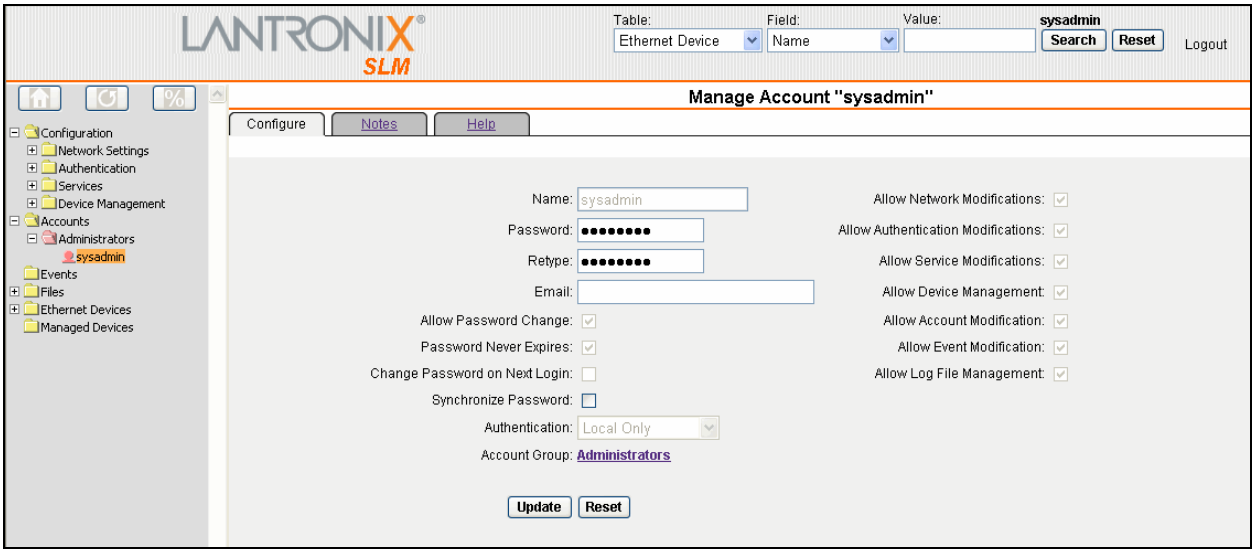
3. To save, click **Apply**.

To change the administrator password:

The default **sysadmin** password is **PASS**.

1. On the menu, click **Accounts→Administrators→sysadmin**. The following page opens:

Figure 3-12. Account Page for sysadmin



2. Enter the new administrator password in **Password** and **(Retype)**. The password can be up to 128 characters and is case sensitive.
3. Click the **Update** button. When the update is complete, a confirmation message displays.

Quick Setup Command

`admin quicksetup`

Syntax

```
admin quicksetup
```

Description

Displays the quick setup script on the CLI; only the sysadmin account can use this command.

Next Steps

After quickly getting the SLM up and running, you can complete the configuration on the web pages.

- To learn more about the interfaces, go to *4: Web and Command Line Interfaces*.
- To continue configuring the SLM for your needs, start with *6: Network and Modem Settings*.

4: Web and Command Line Interfaces

The SLM offers two interfaces for configuring the SLM: a web interface and a command line interface (CLI). This chapter introduces you to both.

Web Interface

A web interface allows the administrator to configure and manage the SLM using most web browsers (Netscape Navigator 6.x and later, Internet Explorer 6.0. and later, Firefox 1.5, with JavaScript enabled).

Note: *Certain features, for example Browse http and Browse https access to some non-Lantronix devices, require IE 7.*

Logging in

To log in to the SLM web interface:

1. Open a web browser (Netscape Navigator 6.x and later, Internet Explorer 6.0. and later, or Firefox 1.5, with JavaScript enabled).
2. In the URL field, type **https://** followed by the IP address of your SLM.
3. To configure the SLM, use **sysadmin** as the user name and **PASS** as the password. (These are the default values.)

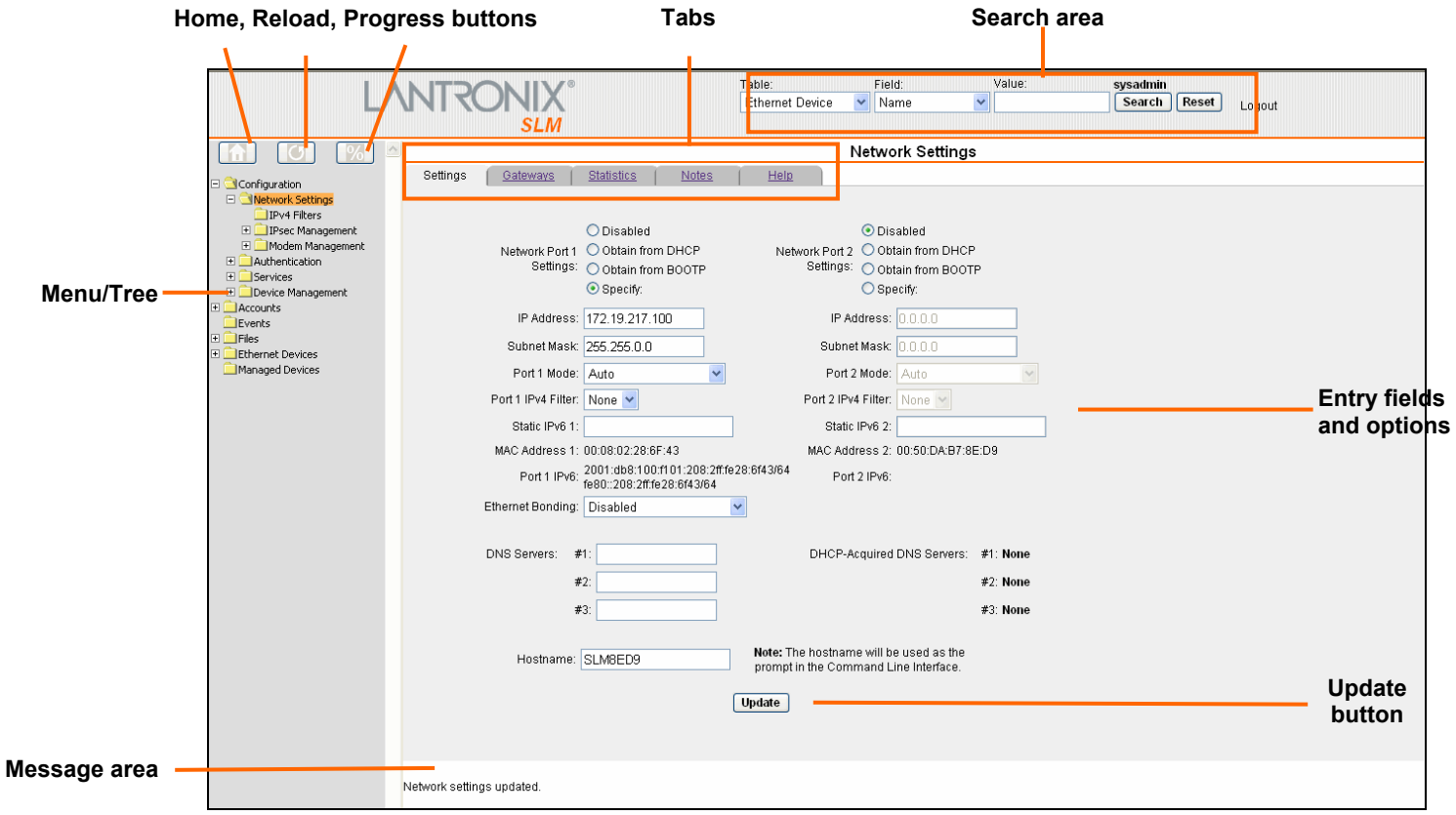
Notes:

- The administrator may have changed the password using the method described in the previous chapter.
- When SecurID is enabled, the user must enter the number on the RSA token. Depending on the state of the user, the login page may require a PIN number, passcode, or new token code.

Typical SLM Web Page

The following figure shows a typical web page:

Figure 4-1. Web Page Layout



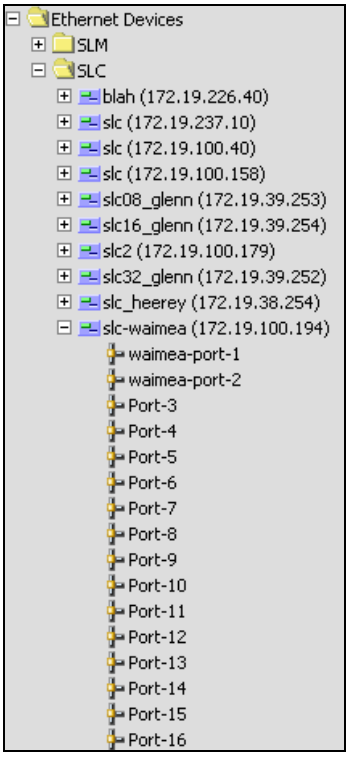
The web page has the following components:

Search Fields: Enable you to search for devices (e.g., SLCs, SLPs, and SLKs), ports, managed devices, and users in the SLM database.

Menu/Tree: Enables you to display a page to configure settings or to perform a function.

- Clicking the expand (plus sign) or contract (minus sign) icon causes the tree structure to toggle between expanded and contracted views but does not populate the page.
- Clicking the folder or document icon causes the tree structure to toggle between expanded and contracted views (for folders) and populates the page.
- Clicking the text only populates the page; the tree structure remains unchanged.

Figure 4-2. Tree Structure on the Menu



Tabs: Display a series of pages related to a particular entity (e.g., account group, network settings, and Ethernet devices).

Home Button: Displays the Lantronix web site home page.

Reload Button: Use to refresh the tree structure after auto-detect, or if some other process (another logged-in user) makes changes that affect the database.

Progress Button: Indicates status of background processes such as bulk updates and automatic detection for SLCs, SLMs, SLKs, SLPs, and SCSs.

Entry Fields and Options: Enable you to enter data and select configuration options.

Update Button: Makes and saves the changes immediately.

Reset Button: Sets field contents to their original values.

Message area: Displays messages such as update confirmations or error messages.

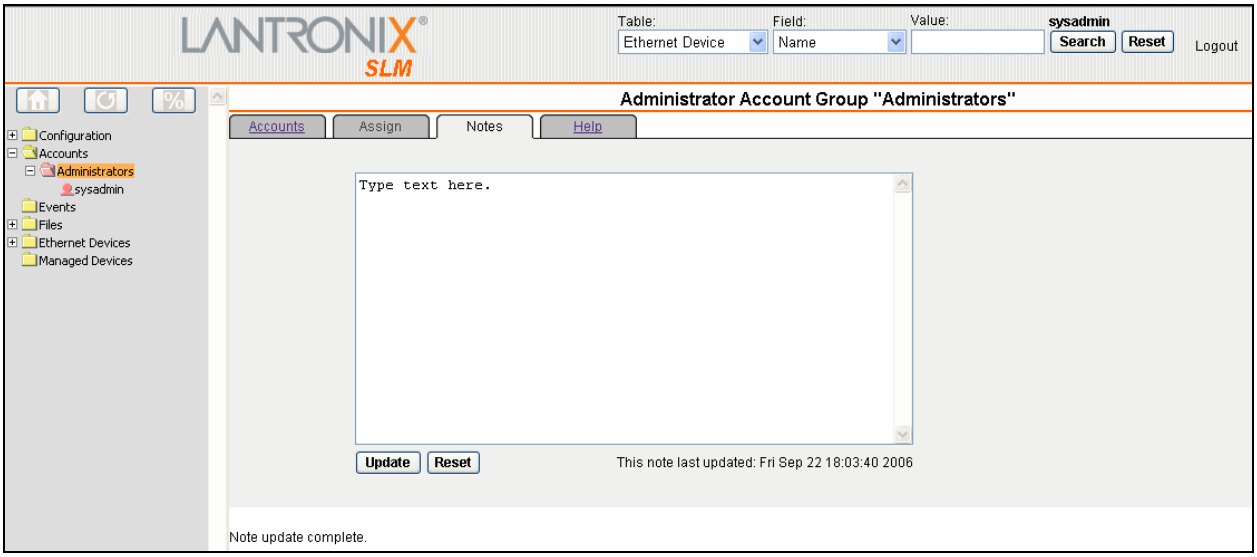
Notes

Administrators and authorized users can add, update, and delete information about any of the entities in the system (e.g., account, account group, device, and event) in the form of a note. All users with permission to view the entity can view notes about it. In this example, we add a note to an account group.

To view, add, update, and delete a note:

1. On the page for the entity to which you want to add a note (e.g., Account Group page), click the **Notes** tab. The following page opens.

Figure 4-3. Note for an Account Group



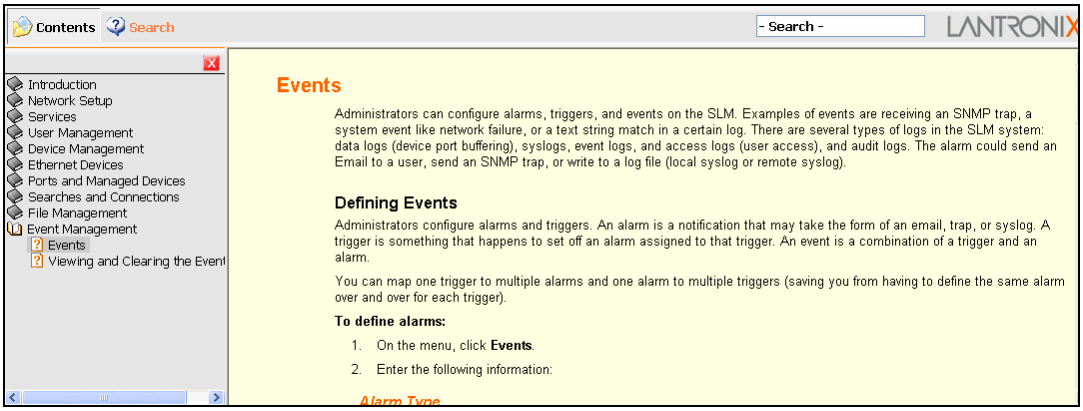
2. In the text box, type the information you want to associate with the entity.
3. Do one of the following:
   - To reset the note to its previous contents, click the **Reset** button.
   - To delete a saved note, click in the box, press **CTRL+A**, press **Delete**, and then click the **Update** button.
   - To save a new note, click the **Update** button. A confirmation message displays. The next time you open the page, it displays the note and the date and time of the update.

Web Page Help

To view detailed information about an SLM web page:

1. Click the **Help** tab. A Help page opens for the tab you are viewing. The **Contents** and **Search** buttons are above the pane on the left.

Figure 4-4. Example of a Help Page


Contents
Search
- Search -
LANTRONIX
Introduction
Network Setup
Services
User Management
Device Management
Ethernet Devices
Ports and Managed Devices
Searches and Connections
File Management
Event Management
Events
Viewing and Clearing the Event
Events
Administrators can configure alarms, triggers, and events on the SLM. Examples of events are receiving an SNMP trap, a system event like network failure, or a text string match in a certain log. There are several types of logs in the SLM system: data logs (device port buffering), syslogs, event logs, and access logs (user access), and audit logs. The alarm could send an Email to a user, send an SNMP trap, or write to a log file (local syslog or remote syslog).
Defining Events
Administrators configure alarms and triggers. An alarm is a notification that may take the form of an email, trap, or syslog. A trigger is something that happens to set off an alarm assigned to that trigger. An event is a combination of a trigger and an alarm.
You can map one trigger to multiple alarms and one alarm to multiple triggers (saving you from having to define the same alarm over and over for each trigger).
To define alarms:
1. On the menu, click Events.
2. Enter the following information:
Alarm Type

To search for information:

1. Click the **Search** button. A search field displays.
2. Enter the word(s) you want to search for and press **Enter**.

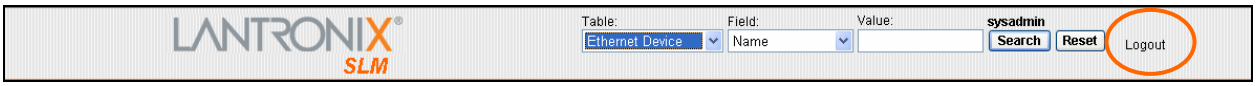
Note: *You can also enter the word in the search field to the left of the Lantronix logo and press* ***Enter.***

Logging out

To log out of the SLM web interface:

1. Click **Logout** to the right of the search buttons on the SLM page banner.

Figure 4-5. Logout on the Page Header



Command Line Interface (CLI)

A command line interface is available for entering the commands for the SLM. You can access the CLI using SSH or a serial terminal connection.

In this User Guide, after each section of instructions for using the web interface, you will find related CLI commands. Not all web page entries have corresponding commands, and vice versa. The **sysadmin** user has access to the complete command set, while all other users have access to a reduced command set.

Logging in

To log in to the SLM command line interface:

1. Do one of the following:
   - With a serial terminal connection, power up, and when the command line displays, press **Enter**.
   - If the SLM already has an IP address (manually assigned previously or assigned by DHCP), SSH to **xx.xx.xx.xx** (the IP address in dot quad notation) and press **Enter**. The login prompt displays.
2. To log in as the administrator for setup and configuration:
   a) Type **sysadmin** as the user name and press **Enter**.
   b) Type **PASS** as the password and press **Enter**.

   Note: *The administrator may have changed the password using the methods described in the previous chapter.*
3. To log in as any other user:
   a) Enter your SLM user name and press **Enter**.
   b) Enter your SLM password and press **Enter**.

Note: When SecurID is enabled, the user must enter the number on the RSA token. Depending on the state of the user, the login page may require a PIN number, passcode, or new token code.

Commands

Commands have the following format:

`<action> <category> <parameter(s)>`

where

`<action>` is set, show, connect, diag, admin, or logout.

`<category>` is a group of related parameters you want to configure or view. Examples are devicegroup, account, and network.

`<parameter(s)>` is one or more name-value pairs in one of the following formats:

`<parameter name> <aa|bb>`	Specify one of the values (aa or bb) separated by a vertical line (|). The values are all lowercase and must be entered exactly as shown. Bold indicates a default value.
`<parameter name> <Value>`	Specify an appropriate value, for example, a device group name. This User Guide shows parameter values in mixed case to indicate they are case sensitive. For example, if you saved a device group name in mixed case, you must enter it in mixed case; if you saved it in lowercase, you must enter it in lowercase.
Square brackets [ ]	Indicate optional parameters.

Figure 4-6. Actions and Category Options

Action	Category
`set`	`network | service | ipfilter | account | accountgroup | auth | | nis | ldap | radius | kerberos | tacacs+ | securid |ethernetdevice | manageddevice | datetime |cli | menu | sshkey | history | modem | dialaccount`
`show`	`network | service | ipfilter | iptables |account| accountgroup | auth | nis | ldap | radius | kerberos | tacacs+ | securid | device | port | ethernetdevice | manageddevice | auditlog |syslog| portlog | traplog | eventlog | sessionlog |datetime | cli | menu | sshkey | history | connection | progress | sysconfig | modem | dialaccount | routing`
`connect`	`device | index | ssh | telnet | terminate`
`diag`	`ping | ping6 | nettrace | arp | traceroute | netstat`
`admin`	`autodetect | locallog | version | productkey | option | config | quicksetup | securechannel | signature | banner | reboot | shutdown | showbootbank | switchbank | copybank`
`logout`	Terminates CLI session.

Command Help

For general command help, type: **help**

For more information about a specific command, type **help** followed by the command, for example:

```
help set network
```

OR

type **?** after the command:

```
set network ?
```

Tips

- Type enough characters to identify the action, category, or parameter name uniquely. For parameter values, type the entire value. For example,

  ```
  set network port 1 state static ipaddr 122.3.10.1 mask
  255.255.0.0
  ```

  can be shortened to:

  ```
  se net po 1 st static ip 122.3.10.1 ma 255.255.0.0
  ```

- Use the **Tab** key to automatically complete action, category, or parameter names. Type a partial name and press **Tab** to complete the name if only one is possible, or to display the possible names if more than one is possible.
- Should you make a mistake while typing, backspace by pressing the **Backspace** key or the **Delete** key, depending on how you accessed the interface. Both keys work if you use VT100 emulation in your terminal access program when connecting to the console port. Use the **left** and **right arrow** keys to move within a command.
- Use the **up** and **down arrows** to scroll through previously entered commands. If desired, select one and edit it. You can scroll through up to 100 previous commands entered in the session.
- When the number of lines displayed by a command exceeds the size of the window (the default is 20), the "`Type more to see the next page`" message displays. To display the next page, type **more** and press **Enter.** You can override the number of lines (or disable the feature altogether) with the `set cli` command.
- To clear an IP address, type **0.0.0.0**.

Logging out

To log out of the SLM command line interface:

1. Type **logout** and press **Enter**.

CLI Commands

The following commands relate to the CLI itself.

set cli terminallines

Syntax

```
set cli terminallines <disable|1-1000>
```

Description

Sets the number of lines that display in a page for the auditlog, syslog, portlog, traplog, and device list. Default is **20**.

set history clear

Syntax

```
set history clear
```

Description

Clears the CLI command history.

show cli

Syntax

```
show cli
```

Description

Displays the terminal lines settings.

show history

Syntax

```
show history
```

Description

Displays the 100 most recent CLI commands.

Session Commands

connect terminate

Syntax

```
connect terminate <connect ID> <one or more parameters>
```

Parameters

```
outbound <outbound ID>
```

You must specify connection ID (inbound ID) to terminate an outbound connection.

Use `show connection` to view the current connections and their ID.

Examples

```
connect terminate 3
```

```
connect terminate 3 outbound 1
```

Description

Terminates a user connection to the SLM session. Use `show connection` to view the current connections and IDs.

show connection

Syntax

```
show connection
```

Description

Displays active user connections and connection IDs.

5: Configuration and Operation Overview

To best use the SLM, review the setup and configuration process outlined below before undertaking the tasks detailed in Chapters 6-10.

Note: *Throughout this user guide, the term "administrator" means the person using the* ***sysadmin*** *user name and those members of the Administrators Account Group permitted to perform the task.*

Following is an overview of the tasks the administrator and other users perform to configure and use the SLM, in roughly the order performed.

The typical user employs SLM as follows:

- Searches for SecureLinx management and other Ethernet devices.
- Connects by browser, SSH, or Telnet to SecureLinx management and other Ethernet devices, and additionally, by secure channel to SLCs and other SLMs.
- Accesses notes and logs about the management devices and their ports.

The administrator performs the following configuration and maintenance activities:

- Updates SLM firmware and configurations.
- Configures properties of the log files.
- Manages syslog, portlog, auditlog, upgrade, configuration, session, and trap files.
- Configures an SNMP agent.
- Configures and views events.
- Updates firmware on Lantronix Ethernet devices (SLM, WiBox, UDS, Spider, SLP, and SLC).

Step 1: Configure Network Settings

The administrator enters the network settings that enable the SLM to access the network, manages modems, and sets up IPv4 filter sets

Step 2: Define Authentication Methods

The SLM supports LDAP, RADIUS, NIS, Kerberos, TACACS+, SecurID, and SSH public key authentication. Remote authentication is optional. The administrator can opt to use only local authentication.

Step 3: Set Up User Account Groups and Accounts

The SLM comes with four types of account groups: Administrators, Ethernet Device, Managed Device, and Menu Only users. Administrators create account groups of each type (except Administrators) and create and assign accounts to the account groups.

The administrator can create additional administrator accounts that have the following rights enabled or disabled:

- Network Settings
- Services (e.g., SNMP and syslog, Date and Time, and Maintenance)
- Authentication
- Accounts
- Events
- Device Management
- File Management

Step 4: Auto-Detect Devices

The administrator uses auto-detection methods to find SecureLinx and other devices on the network and to add them to the SLM database for the SLM to manage. There is no need to add a device manually, although that option is available. Currently, auto-detect supports Lantronix Discovery Protocol (LDP) for SLCs and other Lantronix devices, the Lantronix SCS05/20 device discovery protocol, and SNMP for SLPs, SLKs, and all other Ethernet devices.

Step 5: Associate Account Groups with Ethernet and Managed Devices

Once the SLM administrator adds account groups and Ethernet devices, the next step is to associate the account groups with the Ethernet devices and managed devices (devices attached to Ethernet device's ports) to which they will have access. In the case of SLC/SCS Console Servers, permissions also allow specific account groups listen-only access or full bidirectional control.

Step 6: Manage Devices

The user selects Ethernet devices from the menu's tree structure or enters search criteria to search for Ethernet devices, ports, and managed devices. The user then views port settings (if the device has ports) and can connect to an attached device through a web browser or the CLI.

For ease of communication and management, managed devices that link together device ports (e.g., SLC, SCS, SLK, and SLP) may be created or "fused" together. Users may then manage all of these ports through the managed device on a single web page. In the case of an SLC or another SLM, the user can make a secure channel connection through which the SLM forwards user permission information so a secondary login is not required. For SLCs, once a secure channel has been set up, the user can make a web channel connection.

Step 7: Maintain the SLM

The SLM enables the following maintenance tasks:

SLM Firmware Updates: The administrator updates the SLM firmware.

Auto-Save: The administrator saves the configuration of one SLM on another SLM. If there is a need, the second SLM can "become" the first SLM.

Configuration Save and Restore: The administrator saves and restores system configurations, providing rapid recovery of inadvertent configuration changes.

User Log (Audit Trail): Every successful login, logout, and command on the command line interface and web is logged into a database table. The administrator reads this information from the CLI or web and creates an audit report for one or multiple users.

Events: The administrator defines alarms and triggers that constitute an event. Events are sent to specific users or recorded on the syslog or on another device through an SNMP trap.

Files: The administrator manages (imports, exports, deletes, and renames) and views upgrade, configuration, syslog, audit log, port log, sysconfig, device session, and trap files.

6: Network and Modem Settings

This chapter is primarily for the administrator. It explains how to enter the network configuration, IPv4 filters, and modem settings for the SLM using the SLM web interface or the CLI. If you used a procedure in *3: Quick Setup* to get your unit up and running on the network, you can add or update settings here.

IP Address and Other Required Information

> ***Note:*** *On the SLM-02, both Network Ports 1 and 2 are 10/100/1000Base-T. Previous versions of the SLM have one 10/100Base-T and one 10/100/1000Base-T network port.*

To configure the unit for use on the network, you need the following information:

Network Port 1:

IP address (if not already assigned)**:** _____. _____ . _____ ._____

Subnet mask: _____. _____ . _____ ._____

Network Port 2: (optional)

IP address (if not already assigned)**:** _____. _____ . _____ ._____

Subnet mask: _____. _____ . _____ ._____

Default Gateway: _____. _____ . _____ ._____

DNS Server: _____. _____ . _____ ._____

Your SLM must have a unique IP address on your network. If you assign an IP address manually, **it must be within a valid range and unique to your network.** The administrator generally provides this information.

The SLM receives an IP address in one of the following ways:

Automatically: The first time you power up the SLM, Network Port 1 tries to obtain its IP address automatically through DHCP. If you have connected the network port to a network with a DHCP server, the network port acquires an IP address. Smaller networks may use BOOTP.

Using Detector: Using this software, included on the product CD, you can quickly replace an automatically assigned IP address with a static IP address.

Manually: If the SLM cannot obtain an IP address by means of DHCP, you must manually enter an IP address using a terminal or a PC running a terminal emulation program to the unit's serial console port.

Once the SLM has an IP address, you can configure the remaining settings (and change the IP address, if desired) using the CLI or the web interface.

Using the Web Interface

After the unit has an IP address, you can configure network parameters that determine how the SLM interacts with the attached network and enter the date, time, and timezone.

Note: 4: Web and Command Line Interfaces describes the web interface in detail.

To log in:

1. Open a web browser (Netscape Navigator 6.x and later, Internet Explorer 6.0. and later, or Firefox 1.5, with JavaScript enabled).
2. In the URL field, type **https://** followed by the IP address of your SLM.
3. Log in using **sysadmin** as the user name and **PASS** as the password. The SLM Configuration page opens.

Figure 6-1. SLM Configuration Page

Network Port(s)

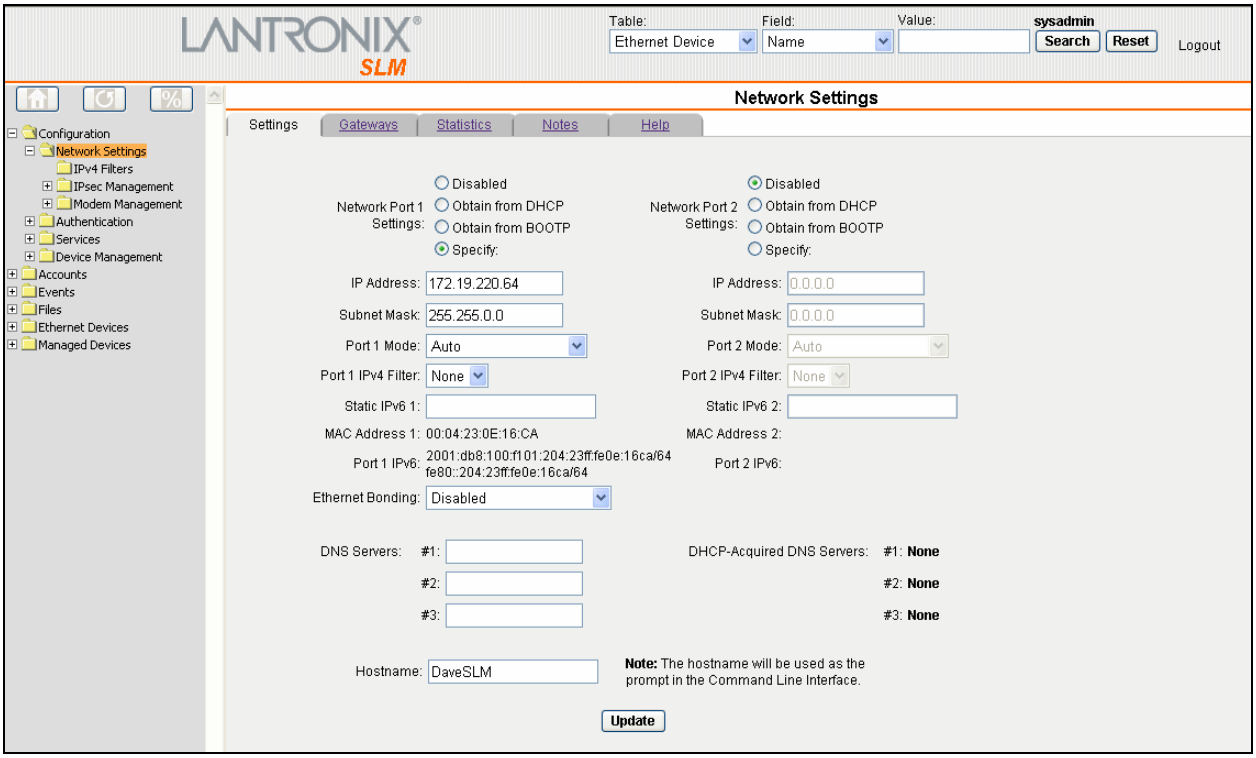
Notes:

- *On the SLM-02, both Network Ports 1 and 2 are 10/100/1000Base-T. Previous versions of the SLM have one 10/100Base-T and one 10/100/1000Base-T network port.*
- *One possible use for the two Ethernet ports is to have one port on a private, secure network, and the other on an unsecured network.*
- *Both Ethernet ports should not be on the same subnet.*

To enter settings for one or both network ports:

1. On the menu, click **Configuration→Network Settings**. The following page opens:

Figure 6-2. Network Settings Page



2. Enter the following information for one or both network ports:

Network Port Settings

Network Port Settings	**Disabled:** This is the default setting for Network Port 2. **Obtain from DHCP:** Acquires IP address, subnet mask, and gateway from the DHCP server. (The DHCP server may provide the gateway, depending on its setup.) This is the default setting for Network Port 1. If you select this option, skip to step 3. **Obtain from BOOTP:** Lets a network node request configuration information from a BOOTP "server" node. Skip to step 3. **Specify**: Requires you to assign a static IP address manually. The administrator generally provides the IP address.
IP Address	If specifying an IP address, enter an IP address that is within a valid range, unique to your network, and in the same subnet mask as your workstation. There is no default. ***Note:** Enter all IP addresses in dot quad notation.*
Subnet Mask	If specifying an IP address, enter the network segment on which the SLM resides. There is no default.
Port mode	The method of data transmission (**Auto**, **Half-Duplex**, or **Full-Duplex**).

Port 1 and Port 2 IPv4 Filter	If you have added filter sets on the IPv4 Filter Definitions page, select the desired one. (See *IPv4 Filters* on page 56.)
Static IPv6	IPv6 addresses are written as 8 sets of 4-digit hexadecimal numbers separated by colons. There are several rules for modifying the address. For example, 1234:0BCD:1D67:0000:0000:8375:BADD:0057 may be shortened to 1234:BCD:1D67::8375:BADD:57. ***Note:*** *The SLM stores all IP addresses internally using IPv6 format. When rendering these addresses for display, the SLM uses IPv4 unless the address cannot be displayed in that format, in which case it uses shortened IPv6.*
MAC Address (display only)	Also referred to as the Hardware or Ethernet address.
Port IPv6 (display only)	IPv6 addresses active on this network port.
Ethernet Bonding	Ethernet bonding is a way of joining two Ethernet interfaces into a single virtual interface for redundancy and/or load balancing. The SLM supports four types of Ethernet bonding in addition to the default state of disabled. ***Note:*** *With bonding enabled, the IP/netmask settings for network port 1 are applied to the virtual bonding interface.* Select one of the following: **Active Backup:** Only one of the two Ethernet interfaces will be active (involved in transmitting and receiving data) at any one time. If the SLM detects that the Ethernet interface has lost network connectivity, the system makes the secondary interface the new active one after a few seconds (~3.5 - 4) of delay. (This delay length is also used with the other bonding settings.) **802.3ad Layer 2:** IEEE 802.3ad-compliant dynamic link aggregation. This is a load-balancing strategy that uses the destination MAC address as the criterion for determining which interface to send each data frame out of. **802.3ad Layer 3+4**: Much like 802.3ad Layer 2, but uses the destination IP and TCP/UDP port number to determine which interface to send data from. ***Note:*** *Both 802.3ad bonding modes require that both network interfaces share the same speed/duplex modes. This rule is currently enforced by the web interface, but not by the CLI.* **Adaptive Load Balancing:** This mode determines which interface to send data from by looking at the current load on each interface. It also controls which interface will receive a response by modifying the SLM's ARP replies before they are sent out. If a link failure occurs on one of the network ports, the system will fail over to the other interface. ***Note:*** *In theory, the active-backup and adaptive load balancing modes do not require any special network switch configuration, while the two 802.3ad modes do. The*

	active-backup mode is recommended for most situations, as redundancy tends to be a more important goal than the relatively small increase in bandwidth (note that bonding two interfaces for load balancing does not double the available bandwidth because of protocol overhead issues).

3. Configure up to three name servers, either by entering the IP addresses or by accepting the IP addresses assigned by DHCP:

DNS Servers

#1	IP address of the primary name server. This entry is required if you choose to configure DNS (Domain Name Server) servers.
#2 (optional)	IP address of the secondary DNS name server.
#3 (optional)	IP address of the tertiary DNS name server.
DHCP-Acquired DNS Servers (view only)	DNS servers automatically assigned by DHCP. The default setting for up to three servers is **None**.

4. Enter the following:

Hostname

Hostname	The default hostname is SLM. You can specify a fully qualified domain name (for example, SLM.lantronix.com). There is a 64-character limit (contiguous characters, no spaces). ***Note:*** *The hostname becomes the prompt in the command line interface.*

5. To save your entries, click the **Update** button.

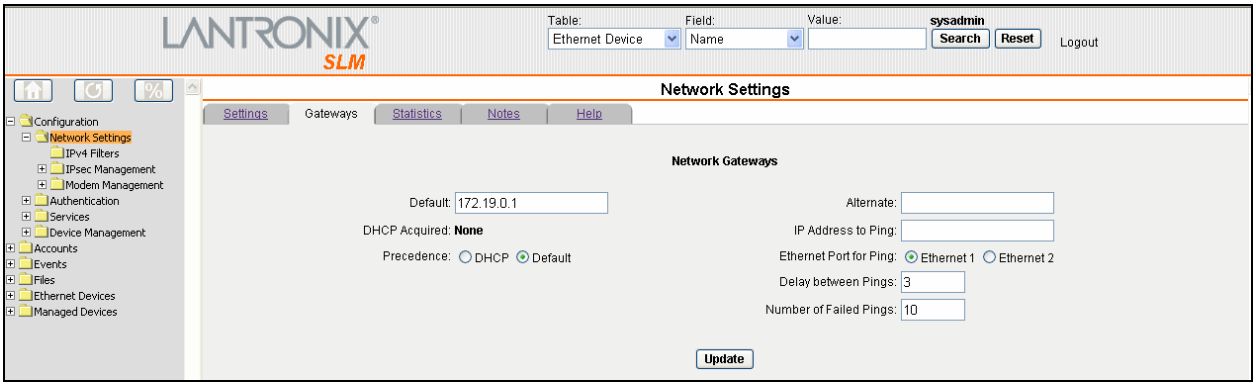
Network Gateways

You can enter network gateway information.

To enter gateway information:

1. On the Network – Settings page, click the **Gateways** tab. The following page opens:

Figure 6-3. Network Settings – Statistics Tab



2. Enter the following:

Default	IP address of the router for this network. If this has not been set manually, any gateway assigned by DHCP for Network Port 1 or Network Port 2 displays. All network traffic that matches the Network Port 1 IP address and subnet mask goes out Network Port 1. All network traffic that matches the Network Port 2 IP address and subnet mask goes out Network Port 2. If you set a default gateway, the SLM sends any network traffic that does not match Network Port 1 or Network Port 2 to the default gateway for routing.
DHCP Acquired (view only)	Gateway assigned by DHCP for Network Port 1 or Network Port 2. The default setting is **None**.
Precedence	Indicates whether the gateway assigned by DHCP or the default gateway takes precedence. The default setting is **DHCP Gateway**. If you select **DHCP Gateway**, and both network ports are configured for DHCP, the SLM gives precedence to the Network Port 1 gateway.
Alternate	An alternate IP address of the router for this network, to be used if an IP address usually accessible through the default gateway fails to return one or more pings.
IP Address to Ping	IP address to ping to determine whether to use the alternate gateway.
Ethernet Port to Ping	Ethernet port to use for the ping.
Delay between Pings	Number of seconds between pings
Number of Failed Pings	Number of pings that fail before the SLM uses the alternate gateway.

3. To save your entries, click the **Update** button.

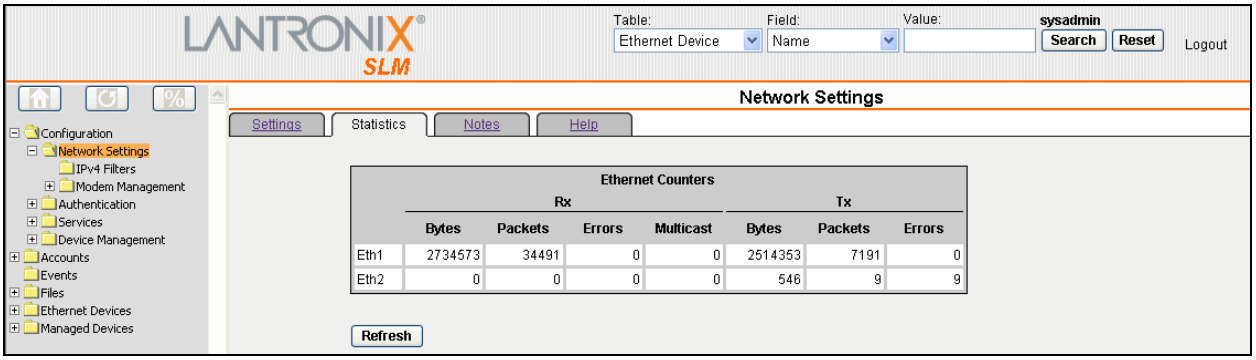
Viewing Network Statistics

You can check Ethernet counters for the network port(s).

To view network statistics:

1. On the Network – Settings page, click the **Statistics** tab. The following page opens:

Figure 6-4. Network Settings – Statistics Tab



Statistics include the following counters for Rx and Tx transmissions:

Bytes	Number of bytes received or transmitted through this Ethernet interface.
Packets	Number of Ethernet packets received or transmitted through the interface.
Errors	Number of received or transmitted packets with physical layer errors.
Multicast (Tx only)	Number of received or transmitted packets with the destination address equivalent to a multicast address.

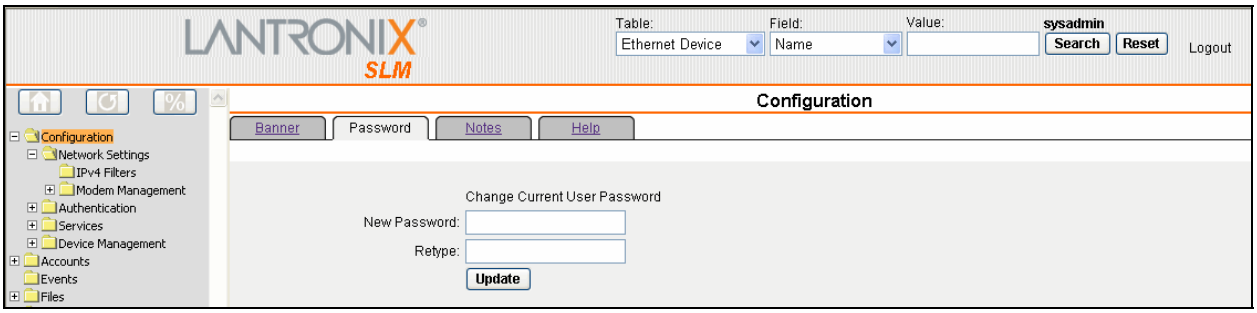
Changing the Current User's Password

Users logged in locally (not using remote authentication) may change passwords at any time, unless the administrator has disabled this option.

To change your password:

1. On the menu, click **Configuration**. The Configuration Home page opens.
2. Click the **Password** tab. The following page opens:

Figure 6-5. Configuration Page – Password Tab



3. Enter the new password in the **Password** and **Retype** fields.
4. Click the **Update** button.

Network Commands

admin quicksetup

Syntax

```
admin quicksetup
```

Description

Displays the quick setup script on the CLI; only the sysadmin account can use this command.

set network dns

Syntax

```
set network dns <1|2|3> ipaddr <IP Address>
```

Description

Configures up to three DNS servers.

set network gateway

Syntax

```
set network gateway <parameters>
```

Parameters

```
default <IP Address>
precedence <dhcp|default>
alternate <IP Address>
pingip <IP Address>
ethport <1 or 2>
pingdelay <1-250 seconds>
failedpings <1-250>
```

Description

Sets the default gateway.

set network host

Syntax

```
set network host <Hostname>
```

Description

Sets the SLM hostname.

set network port

Syntax

```
set network port <1|2> <parameters>
```

Parameters

```
state <dhcp|bootp|static|disable>
```

```
[ipaddr <IP Address> mask <Mask>]
mode <auto|10mbit-half|100mbit-half|10mbit-full|100mbit-full>
[ipfilter <IPv4 Filter Name | CLEAR>]
```

`CLEAR` removes the IP filter assignment.

Description

Configures Network Port 1 or 2.

show network all

Syntax

```
show network all
```

Description

Displays all network settings.

show network port

Syntax

```
show network port <1|2>
```

Description

Displays Network Port 1 and Network Port 2 connection information.

show network settings

Syntax

```
show network settings
```

Description

Displays all network settings.

IPv4 Filters

***Warning:* IPv4 filters configuration is a feature for advanced users. Adding and enabling IPv4 filter sets incorrectly can disable your SLM.**

IPv4 Filters act as a firewall to allow or deny individual or a range of IP addresses, ports, and protocols. On the IPv4 Filter Definitions pages, the administrator defines and edits IPv4 filter sets and displays the current system-recognized filters.

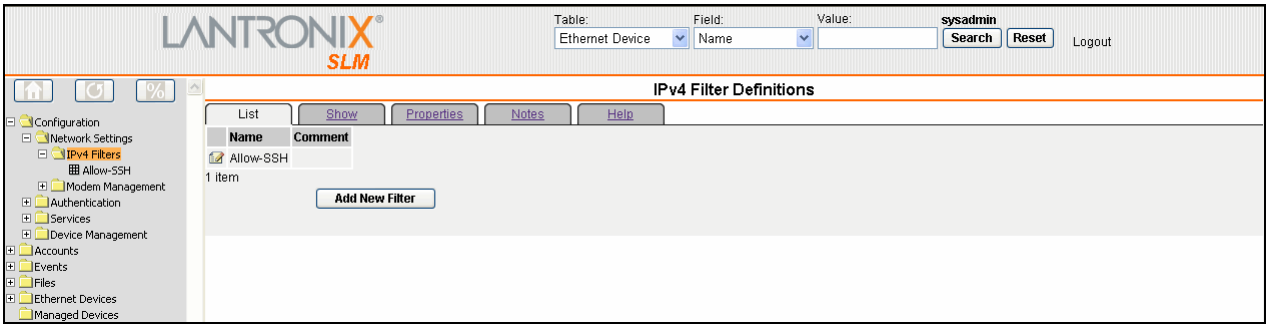
Viewing a List of IPv4 Filters

Each IPv4 filter set is composed of one or more filter rules.

To view a list of available IPv4 filters sets:

1. On the menu, click **Configuration→Network Settings→IPv4 Filters**. The following page displays a list of existing filters.

Figure 6-6. IPv4 Filter Definitions – List Tab



2. View the list of filters and the associated comments.

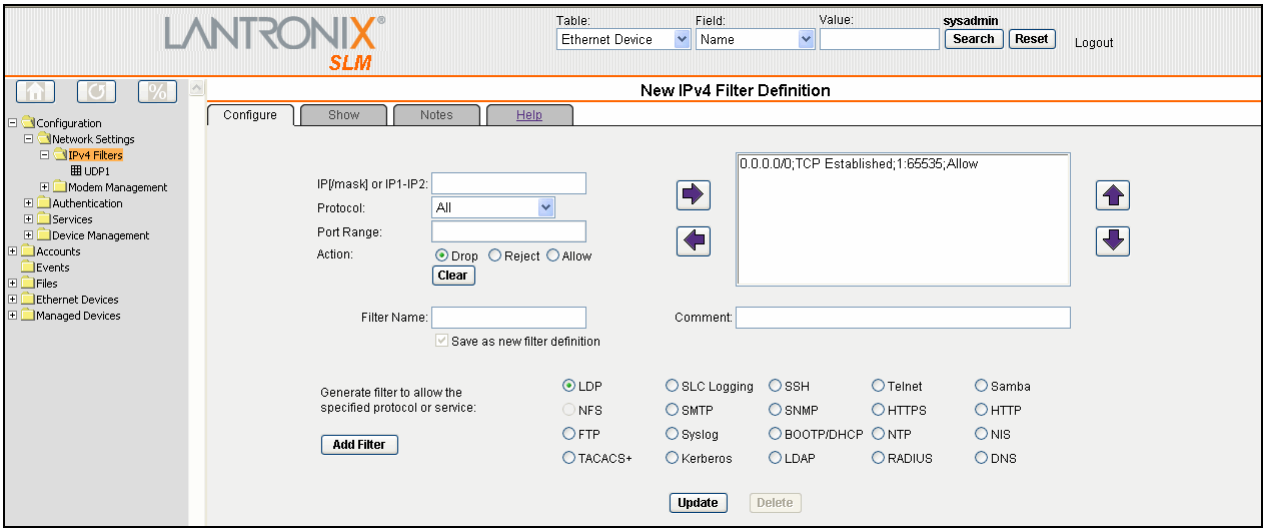
Adding an IPv4 Filter

Note: *User-created IPv4 filter sets display on the menu tree and are composed of one or more filter rules. When a network connection or modem is configured to use an IPv4 filter set, all network traffic through that connection is compared, in order, to the rules of that filter set. Network traffic may be allowed to pass, it may be dropped (without notice), or it may be rejected (sends back an error packet) depending upon the rules of that filter set.*

To add an IPv4 filter:

1. On the **List** tab, click the **Add New Filte**r button. The **Configure** tab displays.

Figure 6-7. New IPv4 Filter Definition – Configure Tab



Note: ***A new filter set is initialized with a rule to allow all established TCP connections. You may remove this rule from your filter set, but do so with caution as loss of connectivity may result.***

2. Enter the following for each filter in the set:

IPv4 Filter

IP[/mask] or IP1-IP2 (optional)	Specify any IP address, IP prefix with mask, or IP range. **Examples:** 172.19.220.64 – this specific IP address only 172.19.0.0/16 – IP addresses 172.19.0.0 – 172.19.255.255 172.19.0.128 – 172.19.64.0 – IP addresses in this range
Protocol	From the drop-down list, select the type of protocol (if any) through which the filter will operate. The default setting is **All**.
Port Range	Enter a range of destination port numbers to be tested. An entry is required for TCP, TCP New, TCP Established, and UDP, and is not allowed for other protocols. Separate multiple ports with commas. Separate ranges of ports by colons. **Examples:** 22 – filter on port 22 only 23,64,80 – filter on ports 23, 64 and 80 23:64,80,143:150 – filter on ports 23 through 64, port 80 and ports 143 through 150
Action	Select whether to drop, reject, or allow communications from IPv4 addresses within the specified range. **Drop** ignores the packet with no notification. **Reject** ignores the packet and sends back an error message. **Allow** permits the packet through the filter.
Filter Name	Name that identifies a filter. The name may be composed of letters, numbers and hyphens only. (The name cannot start with a hyphen.) **Example:** FILTER-2
Save as new filter definition	Select to make small changes to an existing filter set and then save it as a new filter set. If you select this option, you must supply a **Filter Name** that does not already exist.
Comment (optional)	Enter information related to the filter. It displays next to the filter name on the **List** tab.
Generate filter to allow the specified protocol or service	You may wish to "punch holes" in your filter set for a particular protocol or service. For instance, if you have configured your NIS server and wish to create an opening in your filter set, select the **NIS** option and click the **Add Filter** button. This entry adds a new rule to your filter set using the NIS - configured IP address. Other services and protocols added automatically generate the necessary rule to allow their use.

3. Click the **right arrow** button to add the new rule to the bottom of the list box on the right, or click the **Add Filter** button to add a predefined rule to the bottom of the list box.
4. To remove a rule from the filter set, highlight that line and click the **left arrow**. The rule populates the rule definition fields, allowing you to make minor changes before reinserting the rule. To clear the definition fields, click the **Clear** button.

5. To change the order of priority of the rules in the list box, select the rule to move and use the **up** or **down arrow** buttons on the right side of the filter list box.
6. To save, click the **Update** button. A confirmation message displays, and the new filter displays in the menu tree.

Note: *To add another new filter, return to the **List** tab (step 1).*

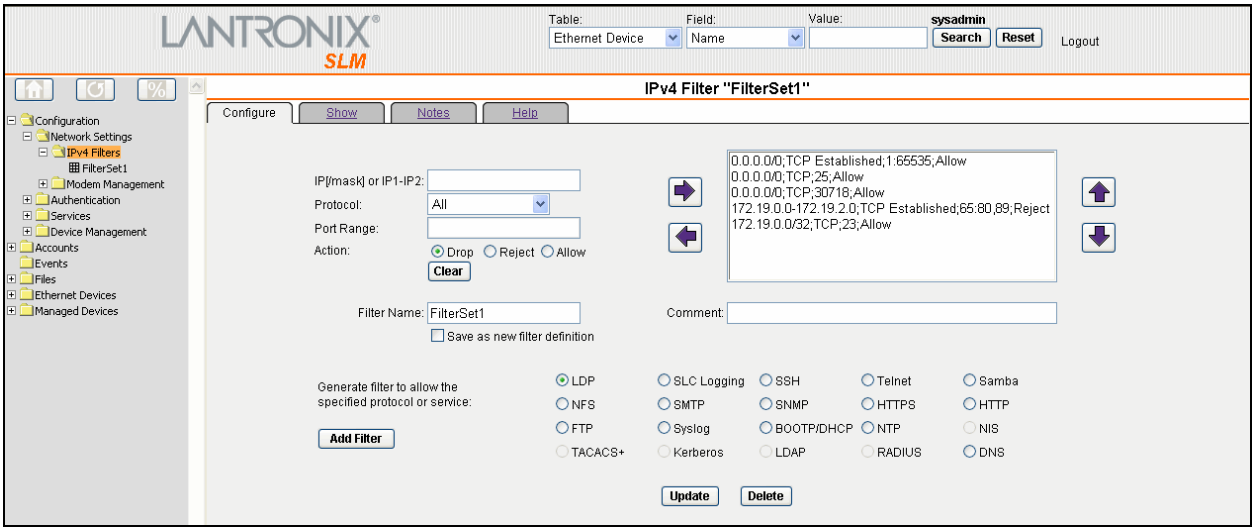
Updating or Deleting an IPv4 Filter

The administrator can update or delete IPv4 filters.

To update or delete an IPv4 filter:

1. On the **List** tab, click the **Edit** icon to the left of the filter. The **Configure** tab displays.

Figure 6-8. IPv4 Filter – Configure Tab



2. To delete a filter:

   Note: *You may not delete a filter set currently referenced by a network interface or a modem.*

   a) Click the **Delete** button.

   b) In response to the request for confirmation, click **OK**.

   c) Click **IPv4 Filters** on the menu tree. The deleted filter is no longer on the menu tree or listed on the **List** tab.

3. To update an IPv4 filter:

   a) Edit the information as desired.

   b) Click the **Update** button. A confirmation message displays.

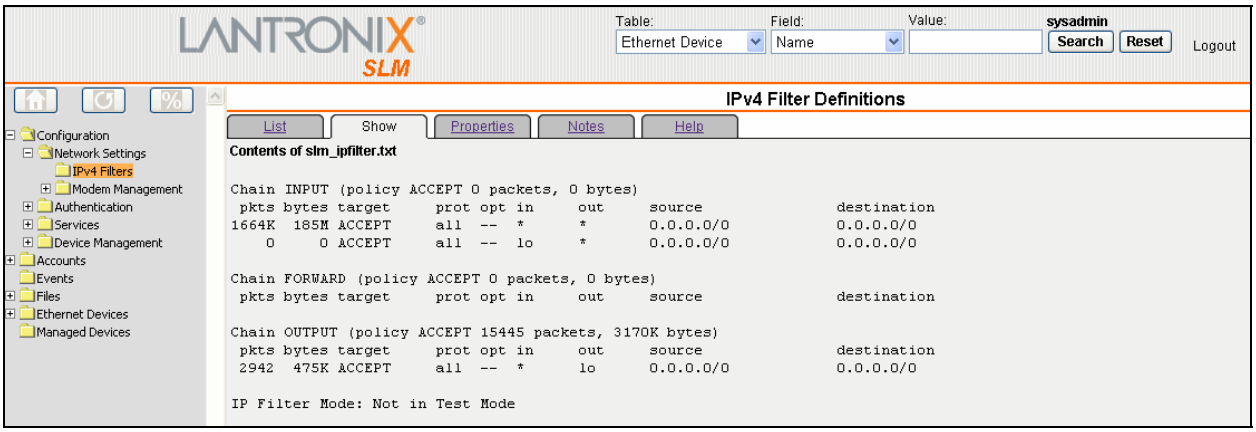
Viewing the System IPv4 Filter Sets

The administrator may view a list of all IPv4 filter sets (user and system) or an individual IPv4 filter set.

To view all filter sets:

1. On the menu, click **IPv4 Filters**. The **List** tab displays.
2. Click the **Show** tab. The following page opens:

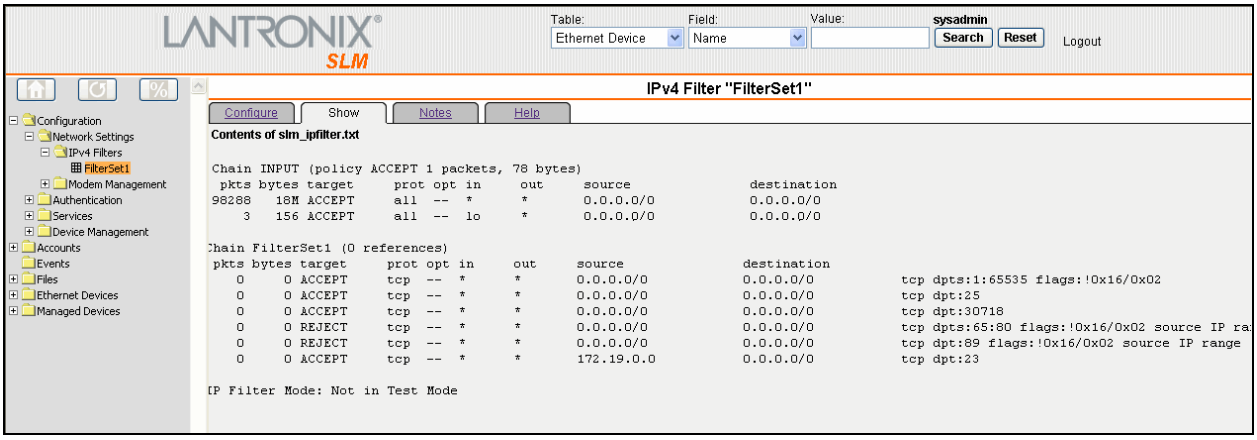
Figure 6-9. IPv4 Filter Definitions – Show Tab



To view an individual IPv4 filter set:

1. On the menu, click the individual filter set name. The IPv4 Filter page for the filter set displays.
2. Click the **Show** tab.

Figure 6-10. IPv4 Filter – Show Tab


LANTRONIX SLM
Table: Ethernet Device
Field: Name
Value:
sysadmin
Search
Reset
Logout
IPv4 Filter "FilterSet1"
Configure
Show
Notes
Help
Contents of slm_ipfilter.txt
Chain INPUT (policy ACCEPT 1 packets, 78 bytes)
pkts bytes target prot opt in out source destination
98288 18M ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0
3 156 ACCEPT all -- lo * 0.0.0.0/0 0.0.0.0/0
Chain FilterSet1 (0 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpts:1:65535 flags:!0x16/0x02
0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:25
0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:30718
0 0 REJECT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpts:65:80 flags:!0x16/0x02 source IP ra
0 0 REJECT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:89 flags:!0x16/0x02 source IP range
0 0 ACCEPT tcp -- * * 172.19.0.0 0.0.0.0/0 tcp dpt:23
IP Filter Mode: Not in Test Mode
Configuration
Network Settings
IPv4 Filters
FilterSet1
Modem Management
Authentication
Services
Device Management
Accounts
Events
Files
Ethernet Devices
Managed Devices

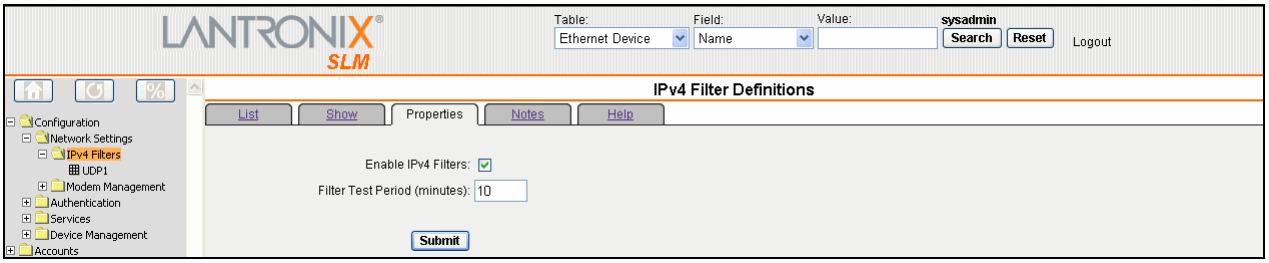
Setting Properties of an IPv4 Filter

For IPv4 filters to be in effect, the **Enable IPv4 Filters** check box must be selected on the **Properties** tab.

To enable and test the IPv4 filter:

1. On the menu, click **IPv4 Filters**. The IPv4 Filter Definitions page displays.
2. Click the **Properties** tab.

Figure 6-11. IPv4 Filter Definitions – Properties Tab



3. Enter the following:

Properties

Enable IPv4 Filters	To enable the filters, select the check box. Disabled by default.
Filter Test Period (minutes)	***Note:*** *There may be times when a complex IPv4 filter set may accidentally lock all users out of the SLM. To allow testing of new filter sets, the administrator can enable and test the filter sets for a specified period.* Before enabling an untested complex filter, enter the number of minutes you would like filters to be active before being automatically disabled. ◆ A zero (0) in this field indicates that filtering will not be automatically disabled, and the **Enable IPv4 Filters** state you specified will take place immediately. ◆ A non-zero value is the number of minutes until IPv4 filters are disabled, **whether or not a lockout condition occurs.** **Example:** You set this value to 5 and enable IPv4 filters. If your system locks up because of a bad filter set definition, then in five minutes, filtering will automatically be disabled. Note that even if there are no problems with the filter set, IPv4 filtering will **still be disabled in 5 minutes**. Once you are satisfied with the IPv4 filter definitions, return to this page and set the **Filter Test Period** to 0 and resubmit to enable IPv4 filtering permanently. ***Note:*** *If you submit a new **Filter Test Period** (larger than 0) when the IP filter is already in test mode, the test timer resets to the new test period and starts test mode again. If you submit a zero **Filter Test Period** when the IP filter is in test mode, the test mode stops, and the specified **Enable IPv4 Filters** state takes effect immediately.* If you have physical access to the SLM, you can always disable IPv4 from the console using the CLI.

4. To save, click the **Submit** button.
5. In response to the confirmation request, click **OK**. A confirmation message displays in the message area.

*Note: To determine whether the IPv4 filter is still in test mode, when the test mode was started, and how long until the test mode ends, click the **Show** tab on the IPv4 Filters page or on an individual IPv4 Filter Set page.*

IPv4 Filter Commands

set ipfilter delete

Syntax

```
set ipfilter delete <Name>
```

Example:

```
set ipfilter delete MyFilter
```

Description

Deletes IPv4 filter set by specified name.

set ipfilter delete all

Syntax

```
set ipfilter delete all
```

Description

Deletes all references to filters.

set ipfilter delete interactive

Syntax

```
set ipfilter delete interactive
```

Description

Deletes IPv4 filters by interactive mode.

set ipfilter name delete

***Note:** Type `show ipfilter name <Name>` or `show ipfilter index <number>` to display the rule number.*

Syntax

```
set ipfilter delete name <Name> [rule <rule number>]
```

Example

```
set ipfilter delete MyFilter rule 3
```

Description

Deletes IPv4 filter rule by specified name and rule number.

set ip filter state

Syntax

```
set ipfilter state <enable|disable>
```

Description

Enables or disables IPv4 filters.

set ipfilter test

Syntax

```
set ipfilter test <number of minutes>
```

Description

Enables or disables IPv4 filter test mode.

show ipfilter

Note: *Type show ipfilter to display index.*

Syntax

```
show ipfilter <parameters>
```

Parameters

```
[name <Filter Name>]
[index <number>]
```

Examples

```
show ipfilter
show ipfilter name MyFilter
show ipfilter index 2
```

Description

Displays IPv4 filter information.

show iptables

Syntax

```
show iptables
```

Description

Displays all IP filtering rules for all chains.

IPsec Management

Internet Protocol Security (IPsec) for the SLM includes IKE policy for internet key exchanges and Virtual Private Network connections.

Internet Key Exchange (IKE) Policies

The administrator can view, add, and update one or more IKE policies.

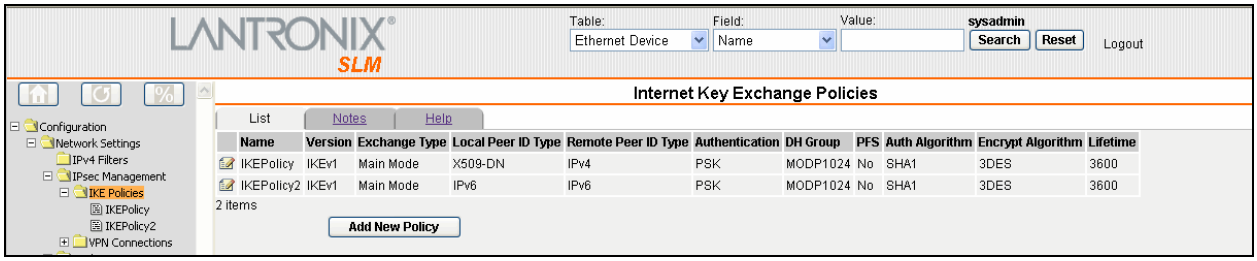
Viewing a List of IKE Policies

The administrator can view IKE Policies.

To view a list of available IKE policies:

1. On the menu, click **IPsec Management → IKE Policies**. The following page displays, listing current IKE policies.

Figure 6-12. Internet Key Exchange Policies Page



2. View the list of policies and associated information:

Name	Name identifying the IKE policy.
Gateway Type	IPv4 or IPv6 type of address.
Authentication	Method of verifying data integrity: **PSK:** Pre-Shared Key uses a password exchange and matching process.
Exchange Type	Mode during the security association phase of the key exchange. ***Note:*** *Aggressive mode will be available in a future release.*
Local Peer ID Type	Local SLM identification type: **IPv4:** Internet Protocol version 4 **IPv6:** Internet Protocol version 6 **FQDN:** Fully Qualified Domain Name **User Email:** Email address of the local user
Remote Peer ID Type	Remote host or gateway identification type.
Certificate	***Note:*** *This feature will be available in a future release.*
PSK Value	The value of a pre-shared key.

PFS	Perfect Forward Secrecy (PFS) ensures that a given IPsec SA key was not derived from any other secret, such as another key. Enabled by default.
DH Group	Diffie-Hellman key group (DHx) used for an encryption key.
Authentication Algorithm	From the drop-down list, select an algorithm for verifying data integrity: SHA1: Secure Hash Algorithm 1 MD5: Message Digest SHA2-256: 256-bit Secure Hash Algorithm
Encryption Algorithm	Method of encrypting data, in order of security level provided: 3DES: Data Encryption Standard AES : Advanced Encryption Standard AES-192: 192-bit key with AES encryption AES-256: 256-bit key with AES encryption
Lifetime	Duration in seconds before a key expires.
Login	Username for XAUTH.
Password	Password for XAUTH.

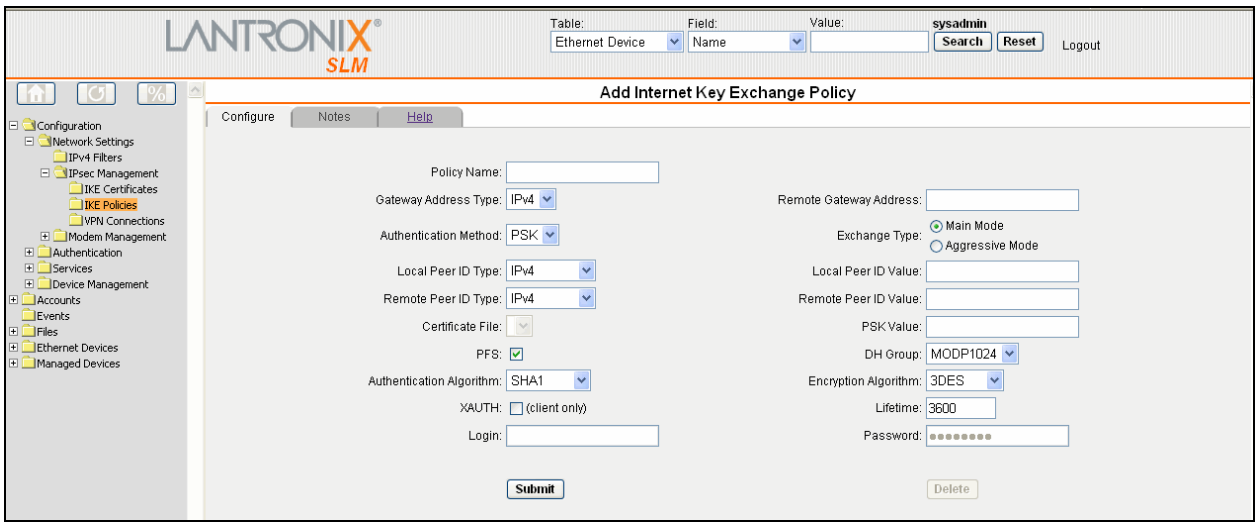
Adding an IKE Policy:

The administrator can add an IKE policy.

To add a new IKE policy:

1. On the **List** tab, click the **Add New Policy** button. The **Configure** tab displays.

Figure 6-13. New IPv4 Filter Definition Page



2. Enter the following information:

Policy Name	Enter a name to identify the IKE policy.
Gateway Address Type	From the drop-down list, select the version of the Internet Protocol used for the address: **IPv4:** Internet Protocol version 4 (default) **IPv6:** Internet Protocol version 6
Remote Gateway Address	Enter the IP address of the remote end of the gateway.
Authentication Method	From the drop-down list, select the method of verifying data integrity: **PSK:** Pre-Shared Key uses a password exchange and matching process. (default) **RSA** Signature: Uses a private and public key that together comprise a digital signature. ***Note:*** *This feature will be available in a future SLM release.*
Exchange Type	Select the mode during the security association phase of the key exchange: **Main Mode:** (default) ***Note:*** *Aggressive mode will be available in a future release.*
Local Peer ID Type	From the drop-down list, select the method of filtering incoming data. I**Pv4:** Internet Protocol version 4 **IPv6**: Internet Protocol version 6 **FQDN:** Fully Qualified Domain Name **User Email:** Email address of the local user
Local Peer ID Value	Enter the local SLM identification value. This value depends on the Local Peer ID Type setting.
Remote Peer ID Type	Select the method of filtering outgoing data: **IPv4:** Internet Protocol version 4 (default) I**Pv6:** Internet Protocol version 6 **FQDN:** Fully Qualified Domain Name **User Email:** Email address of the remote user
Remote Peer ID Value	Enter the identification value of the remote host or gateway.
Certificate File	***Note:*** *This feature will be available in a future release.*
PSK Value	Enter the value of a pre-shared key.
PFS	Select the checkbox to enable PFS (Perfect Forward Secrecy). PFS ensures that a given IPsec SA key was not derived from any other secret, such as another key. Enabled by default.
DH Group	Initial Diffie-Hellman value.

Authentication Algorithm	From the drop-down list, select an algorithm for verifying data integrity: **SHA1:** Secure Hash Algorithm 1. **MD5**: Message Digest 5. **SHA2-256:** 256-bit Secure Hash Algorithm
Encryption Algorithm	From the drop-down list, select the method of encrypting data (listed below in order of security level provided): **3DES:** Data Encryption Standard **AES:** Advanced Encryption Standard **AES-192:** 192-bit key with AES encryption **AES-256:** 256-bit key with AES encryption
XAUTH	Select to use a "group" shared secret rather than digital certificates for authentication. Disabled by default. ***Note:*** *This feature will be available in a future SLM release.*
Lifetime	Enter the duration in seconds before a key expires. Default is 3600.
Login	Enter the username for XAUTH.
Password	Enter the password for XAUTH.

3. To save your entries, click the **Submit** button.

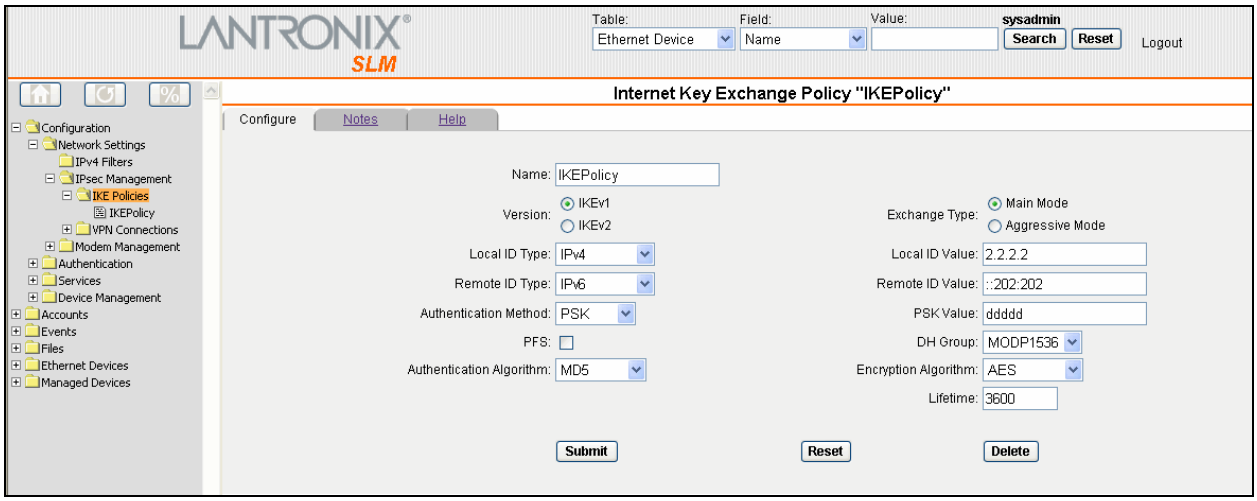
Updating or Deleting an IKE Policy

The administrator can update or delete IKE policies.

To update or delete a policy:

1. On the **List** tab, click the **Edit** icon to the left of the policy. The **Configure** tab displays.

Figure 6-14. Internet Key Exchange Policiy -- Configure Tab



2. To delete a policy:

Note: *You may not delete a policy currently referenced by a VPN.*

a) Click the **Delete** button.

b) In response to the request for confirmation, click **OK**.

c) Click **IKE Policies** on the menu bar.

3. To update a policy:

a) Edit the information as desired.

b) Click the **Update** button. A confirmation message displays.

4. To save your entries, click the **Save** button.

VPN Connections

The administrator can view, add, or update one or more Virtual Private Networks (VPNs). Each VPN must reference an IKE Policy. You can only delete an IKE Policy that is not referenced by a VPN.

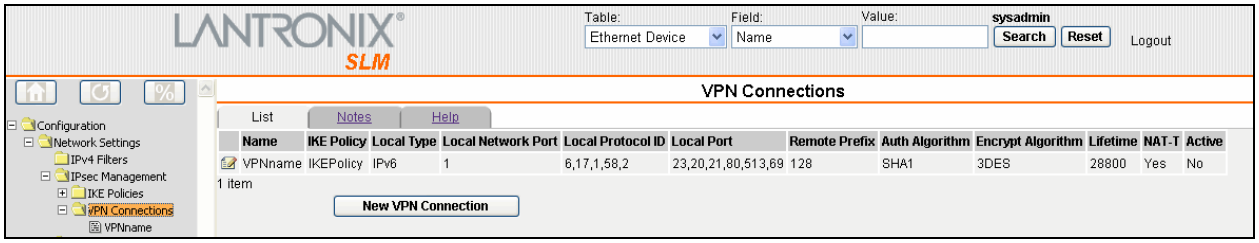
Viewing a List of VPNs

The administrator can view a list of VPNs.

To view a list of VPNs:

1. On the menu, click **Configuration→Network Settings→ IPsec Management → VPN Connections**. The following page displays:

Figure 6-15. VPN Connections Page



2. View the following information about each VPN:

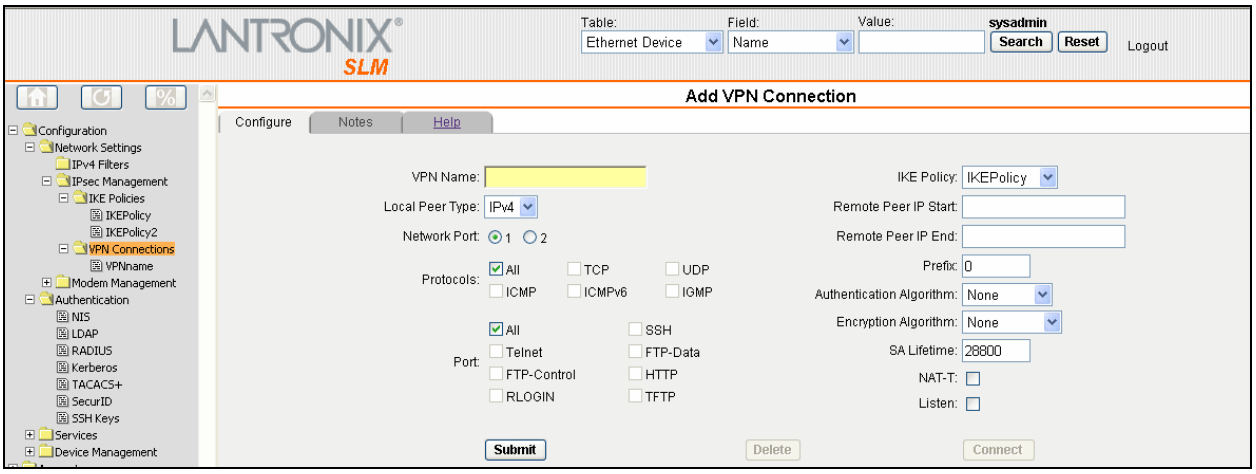
Name	Name that identifies VPN.
IKE Policy	IKE policy that references this VPN.
Encapsulation Mode	**Tunnel mode:** Used when the remote peer is an IPSec gateway. **Host mode:** Used when the remote peer is an IPsec host.
Remote Address Type	**Subnet type:** The subnet that is the destination of the IPsec traffic. **Single:** The single host that is the destination of the IPsec traffic.
Network Port	Network port on the SLM that connects to the VPN.
Local Protocol	IP protocol selected to protect data traffic.
Local Port	Method selected to protect data traffic on the TCP port of the SLM.
Subnet Prefix	Subnet prefix length for Subnet type clients.

Auth Algorithm	Algorithm for verifying data integrity.
Encrypt Algorithm	Method of encrypting data, in ascending order of security level provided: **3DES (Data Encryption Standard)** **Advanced Encryption Standard (AES)** **AES-192: 192-bit key with AES encryption** **AES-256: 256-bit key with AES encryption**
Lifetime	Duration in seconds before a key expires.
Active	Indicates whether the VPN is ready to be connected.
Status	Indicates whether the VPN is connected or disconnected.

Adding a VPN

Administrators may add VPNs.

1. On the **List** tab, click the **New VPN Connection** button. The **Configure** tab displays.



VPN Name	Enter a name to identify the VPN.
Encapsulation Mode	Tunnel mode: Used when the remote peer is an IPSec gateway. Host mode: Used when the remote peer is an IPsec host.
Network Port	Select the network port connecting to the VPN.

Protocols	Select the protocol used in the VPN connection: ALL: All of the listed protocols are used. TCP: Transmission Control Protocol UDP: User Datagram Protocol ICMP: Internet Control Message Protocol ICMPv6: Internet Control Message Protocol version 6 IGMP: Internet Group Management Protocol
Port	Select the type of security used on the port: **All** **SSH** **Telnet** **FTP Data** **FTP Control** **HTTP** **RLOGIN** **TFTP**
IKEPolicy	IKE Policy that references this VPN.
Remote Peer Address Type	**Subnet type:** The subnet that is the destination of the IPsec traffic. **Single:** The single host that is the destination of the IPsec traffic.
Remote Peer IP Start	Starting IP address in a range of remote IP addresses.
Subnet Prefix	Prefix of the subnet for Subnet Type peers.
Authentication Algorithm	From the drop-down list, select the algorithm for verifying data integrity: **None** **SHA1**: **MD5**: **SHA2-256**:
Encryption Algorithm	From the drop-down list, select the method of encrypting data: **3DES (Data Encryption Standard**) **AES** **AES-192** **AES-256**
SA Lifetime	Duration in seconds before an IPsec Security Association (SA) expires. The default is 28800.
Active	Select to activate the VPN.

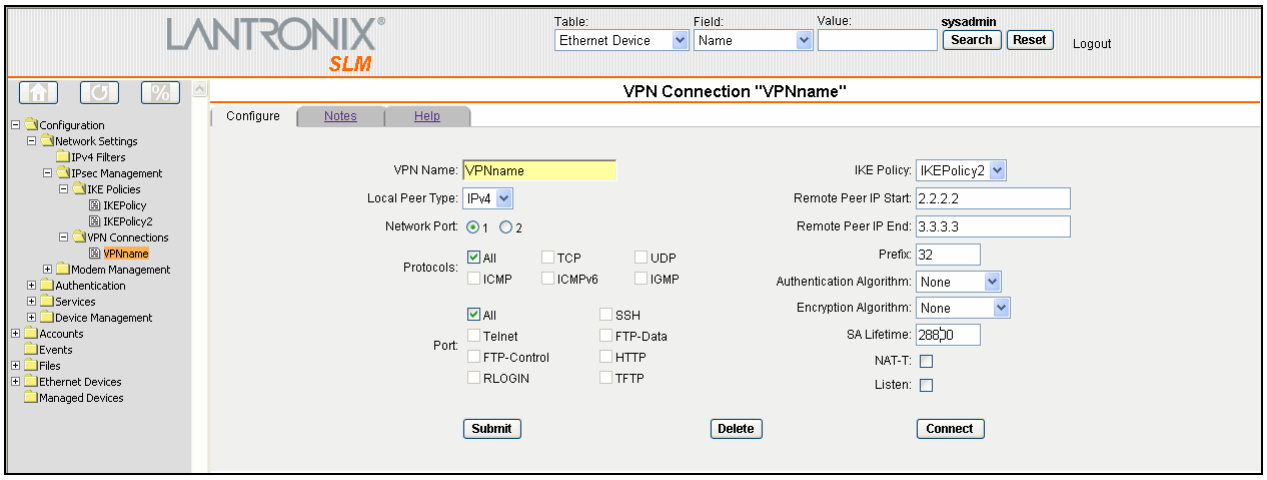
2. To save, click the **Submit** button.

Updating or Deleting a VPN

To update or delete a VPN:

1. On the **List** tab, click the **Edit** icon to the left of the policy. The **Configure** tab displays.

Figure 6-16. VPN Connection -- Configure Tab

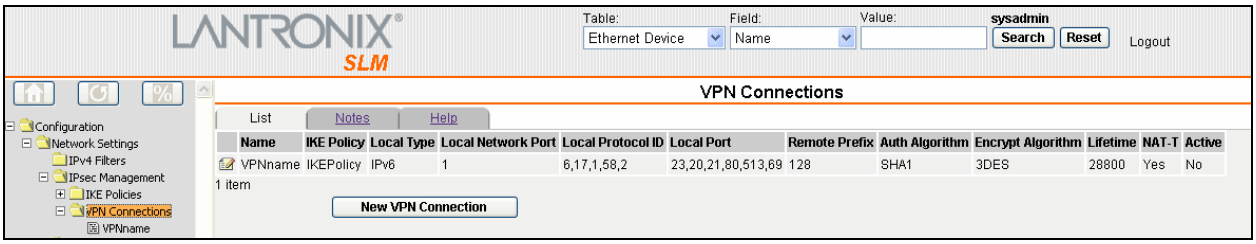


2. To delete a VPN:
   a) Click the **Delete** button.
   b) In response to the request for confirmation, click **OK**.
   c) Click **VPN Connections** on the menu bar.
3. To update a policy:
   a) Edit the information as desired.
   b) Click the **Update** button. A confirmation message displays.
4. To save your entries, click the **Save** button.

Connecting a VPN

To connect a VPN:

1. On the **List** tab, click the **Edit** icon to the left of the VPN. The VPN Connection page displays.



2. Make sure you have updated the connection.
3. Select the **Active** checkbox (if not already selected).
4. Click the **Connect** button. It will take a couple of seconds before the connection is established.

Modem Management

Dial-up modem support ensures access when the network is not available. SLM supports dial-in (text mode and PPP mode) and dial-out (PPP mode) as follows:

- The administrator can configure dial-in and dial-out from either the web interface or the CLI.
- A user dialing in from a remote computer in text mode can access the CLI on the SLM.
- A user dialing in from a remote computer in PPP mode can access the CLI and the web interface on the SLM. Depending on the PPP settings, the user may access all devices that the SLM has access to as well.
- A user can dial out from the CLI and the web interface in PPP mode.

Viewing a List of Modems

The administrator can view a list of the SLM's internal and external modems.

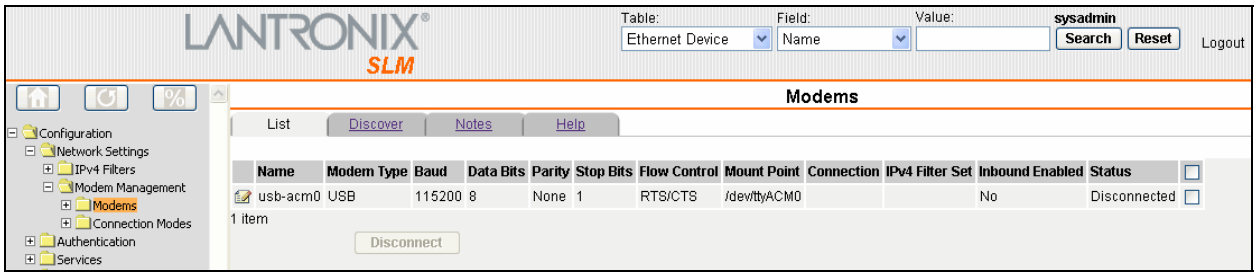
Note: *Currently, the SLM supports PCI and USB modems. (See Discovering a USB Modem on page 79.) The SLM does not support plug-and-play.*

To view a list of available modems:

1. On the menu, click **Configuration→Network Settings→Modem Management→Modems**.

   The following page displays.

Figure 6-17. Modems Page



2. View the following information about each modem:

Name	Name that identifies the modem.
Modem Type	Identifies the type of modem (e.g., PCI or USB).
Baud	Communication speed between the SLM and a modem.
Data Bits	Number of data bits used to transmit a character.
Parity	Type of parity checking. Parity checking detects simple, single-bit errors.
Stop Bits	Number of stop bit(s) used to indicate that a byte of data has been transmitted.
Flow Control	Method of preventing buffer overflow and loss of data.

Mount Point	Name of the serial interface device to which the modem is assigned.
Connection	Name of connection assigned for dial-in. *(See Enabling or Disabling Dial-in Connections on page 74.)*
IPv4 Filter Set	IPv4 filter being used.
Inbound Enabled	Indicates whether the modem is enabled to receive dial-in calls.
Status	Indicates whether the modem is currently connected.

3. To disconnect a connection, select its check box and click the **Disconnect** button.

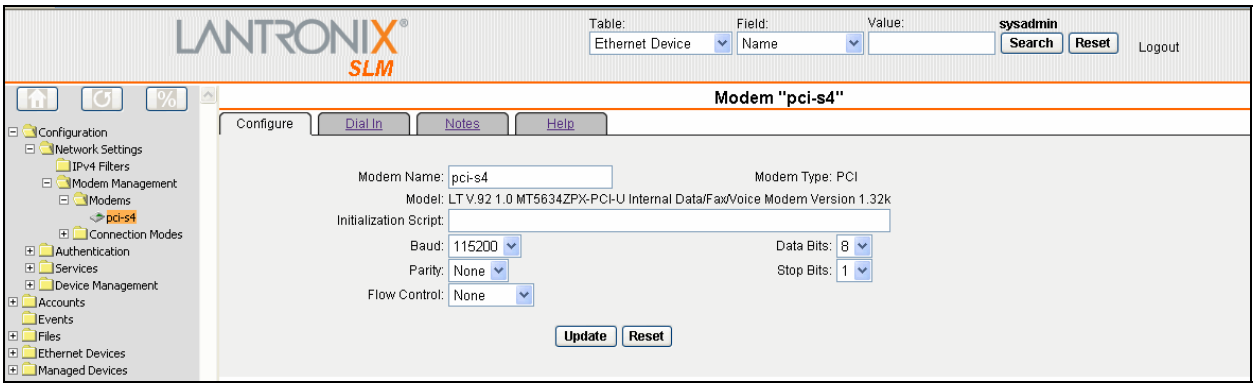
Configuring a Modem

The administrator can configure the modem for an incoming connection from a remote device or computer.

To configure a modem:

1. Select the modem and click the **Configure** tab. The following page opens:

Figure 6-18. Modem Page – Configure Tab



2. Enter the following information:

***Note:** In most cases, you do not need to change these settings.*

Modem Name	You may change the modem name assigned by the SLM.
Modem Type (view only)	Displays **PCI** or **USB**.
Model (view only)	Manufacturer's name for the modem.

Initialization Script	Commands sent to configure the modem may have up to 100 characters. Consult your modem's documentation for recommended initialization options. If you do not specify an initialization script, the SLM uses a default initialization string of **AT S7=45 S0=0 V1 X4 &D2 &C1 E1 Q0**. ***Note:*** *We recommend that the modem initialization script always be preceded with* ***AT*** *and include* ***E1 V1 x4 Q0*** *so that the SLM can properly control the modem.*
Baud	Communication speed between the SLM and the modem. From the drop-down list, select the baud rate. The default setting is **115200.**
Data Bits	Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is **8** data bits.
Parity	Parity checking detects simple, single-bit errors. From the drop-down list, select the parity. The default is **none**.
Stop Bits	Number of stop bit(s) used to indicate that a byte of data has been transmitted. From the drop-down list, select the number of stop bits. The default is **1**.
Flow Control	Method of preventing buffer overflow and loss of data. The available methods include **none**, **XON/XOFF** (software), and **RTS/CTS** (hardware). The default is **RTS/CTS**.

3. To save, click the **Update** button. A confirmation message displays.

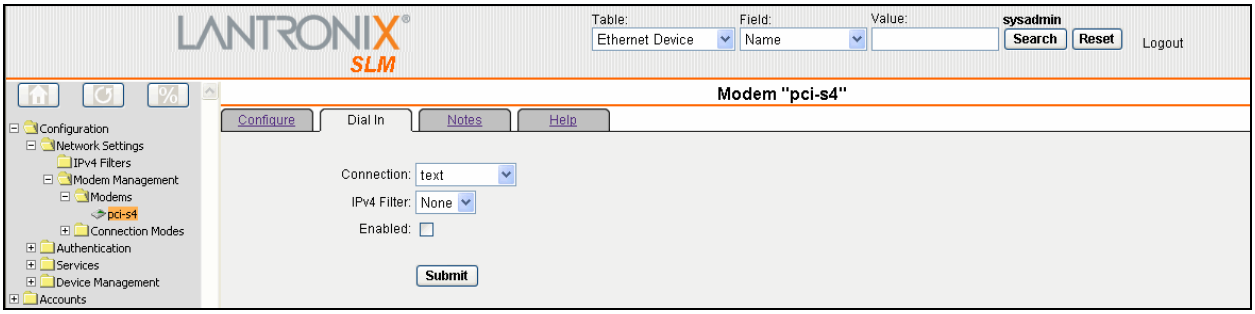
Enabling or Disabling Dial-in Connections

The system administrator can enable the modem to answer incoming calls and can set the mode to use when establishing these connections.

To enable or disable dial-in connections to a modem:

1. Click the **Dial in** tab. The following page opens:

Figure 6-19. Modem Page – Dial in Tab



2. Enter the following information:

Connection	From the drop-down list, select the desired connection. The default is **text**.
IPv4 Filter	From the drop-down list, select an IPv4 filter for the connection. The default is **none**.
Enabled	Select this check box to allow incoming connections on this modem. Disabled by default.

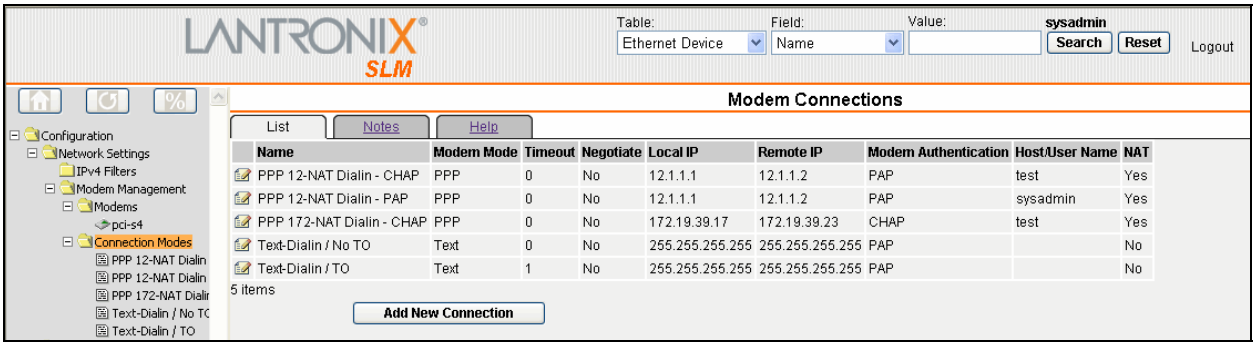
3. To save, click the **Submit** button. A confirmation message displays.

Viewing a List of Connections

The administrator can view a list of modem connections.

1. On the menu, click **Configuration→Network Settings→Modem Management→Connection Modes**. The following page opens:

Figure 6-20. Modem Connections – List Tab


LANTRONIX
SLM
Table:
Ethernet Device
Field:
Name
Value:
sysadmin
Search
Reset
Logout
Configuration
Network Settings
IPv4 Filters
Modem Management
Modems
pci-s4
Connection Modes
PPP 12-NAT Dialin
PPP 12-NAT Dialin
PPP 172-NAT Dialir
Text-Dialin / No TC
Text-Dialin / TO
Modem Connections
List
Notes
Help
Name | Modem Mode | Timeout | Negotiate | Local IP | Remote IP | Modem Authentication | Host/User Name | NAT
PPP 12-NAT Dialin - CHAP | PPP | 0 | No | 12.1.1.1 | 12.1.1.2 | PAP | test | Yes
PPP 12-NAT Dialin - PAP | PPP | 0 | No | 12.1.1.1 | 12.1.1.2 | PAP | sysadmin | Yes
PPP 172-NAT Dialin - CHAP | PPP | 0 | No | 172.19.39.17 | 172.19.39.23 | CHAP | test | Yes
Text-Dialin / No TO | Text | 0 | No | 255.255.255.255 | 255.255.255.255 | PAP | | No
Text-Dialin / TO | Text | 1 | No | 255.255.255.255 | 255.255.255.255 | PAP | | No
5 items
Add New Connection

2. View the following information about each connection:

Name	A name identifying the specific connection.
Modem Mode	The format in which the data flows back and forth: **Text:** In this mode, the SLM assumes that the modem is for remotely logging into the CLI. Text mode is only for dialing in. **PPP:** This mode establishes an IP-based link over the modem. Dial-out mode uses PPP connections (e.g., the SLM connects to an external network). You can dial out from both the CLI and the web interface.
Timeout	Indicates whether the connection times out logins after the connection is inactive for a specified number of minutes (1-30).
Negotiate	If **Yes**, the remote device or PC specifies the local (SLM) IP and remote addresses. If **No**, the SLM assigns the local (SLM) IP and remote IP addresses.
Local IP	IP address of the SLM.

Remote IP	IP address of the remote device or remote PC.
Modem Authentication	Indicates whether the SLM uses **PAP** or **CHAP** to authenticate modem logins.
Host/User Name	Username for dial-ins or dial-outs between the SLM and a remote system.
NAT	If **Yes,** the SLM uses Network Address Translation (NAT) for dial-in PPP connections. Users dialing into the SLM access the network connected to Eth1 and/or Eth2. ***Note:*** *This does not apply to dial-out PPP.*

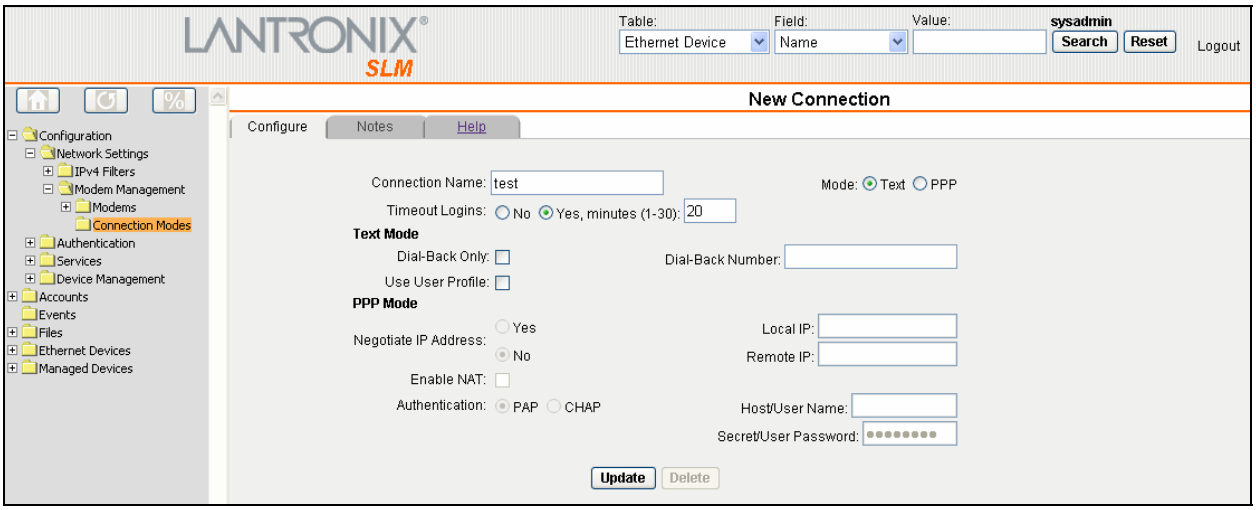
Adding a Connection

The administrator can define a text or PPP connection for use by an appropriate modem in the system.

To add a connection:

1. On the menu, click **Configuration→Network Settings→Modem Management→Connection Modes**, and then click the **Add New Connection** button. The following page opens:

Figure 6-21. New Connection—Configure Tab



2. Enter the following information:

Connection Name	A name identifying the specific connection.
Mode	The format in which the data flows back and forth: **Text:** In this mode, the SLM assumes that the modem is for remotely logging into the CLI. Text mode is only for dialing in. Enabled by default. **PPP:** This mode establishes an IP-based link over the modem. Dial-out mode uses PPP connections (e.g., the SLM connects to an external network). You can dial out from both the CLI and the web interface.

Timeout Logins	For both Text and PPP modes, you can enable logins to time out after the connection is inactive for a specified number of minutes (1-30).

Text Mode

Dial-Back Only	Select to grant a local user dial-back access. Users with dial-back access can dial into the SLM and enter their login and password. Once the SLM authenticates them, the modem hangs up and dials them back. Disabled by default. Following are the rules the SLM follows concerning **Dial-Back Only** in **Text** mode. If both **Dial-Back Only** and **Use User Profile** are not selected, users can dial in text mode. (Regular usage). If **Dial-Back Only** is not selected and **Use User Profile** is selected: ◆ If **Enable Dial-back** is selected on the Manage Account page, the user can only dial in using dial-back with the number defined on the Manage Account page. ◆ If **Enable Dial-back** is not selected, the user can dial in using text mode. If **Dial-Back Only** is selected and **Use User Profile** is not selected, users can only dial in using dial-back. SLM dials back to the number defined on the Modem Connection. If **Dial-Back Only** is selected and **Use User Profile** is selected ◆ If **Enable Dial-back** on the Manage account page is selected, the user can only dial in using dial-back with the number defined on the Manage account page. ◆ If **Enable Dial-back** on the Manage account page is **not** selected, the user can only dial in using dial-back. SLM dials back to the number defined on the Modem connection page.
Dial-Back Number	Enter the phone number the modem dials back on. It can be a fixed number or a number associated with the user's login. If you select **Fixed Number**, enter the number in the format 2123456789.
Use User Profile	Select to indicate that the SLM takes dial-back rules from the local user account on the Manage Account page (see *Accounts* on page 109).

PPP Mode

Negotiate IP Address	For the remote device or PC to specify the local (SLM) IP and remote addresses, select **Yes**. Defaults to **Yes.** For the SLM to assign the local (SLM) IP and remote IP addresses, select **No,** and enter the local IP (IP address of the SLM) and remote IP (IP address of the remote device or PC).
Local IP	IP address of the SLM.
Remote IP	IP address of the remote device or remote PC.
Enable NAT	Select to enable Network Address Translation (NAT) for dial-in PPP connections. Users dialing into the SLM access the network connected to Eth1 and/or Eth2. ***Note:*** *This does not apply to dial-out PPP.*
Authentication	Enables **PAP** or **CHAP** authentication for modem logins. **PAP** is the default. ◆ With PAP, if you do not specify username and password, users are authenticated by means of the Local Users and any of the remote authentication methods that are enabled. ◆ With CHAP, the CHAP Handshake fields authenticate the user. You must specify the username and password.
Host/User Name	User name for dial-ins or dial-outs between the SLM and a remote system for PAP or CHAP authentication.
Secret/User Password	Password for dial-ins or dial-outs between the SLM and a remote system for PAP or CHAP authentication.

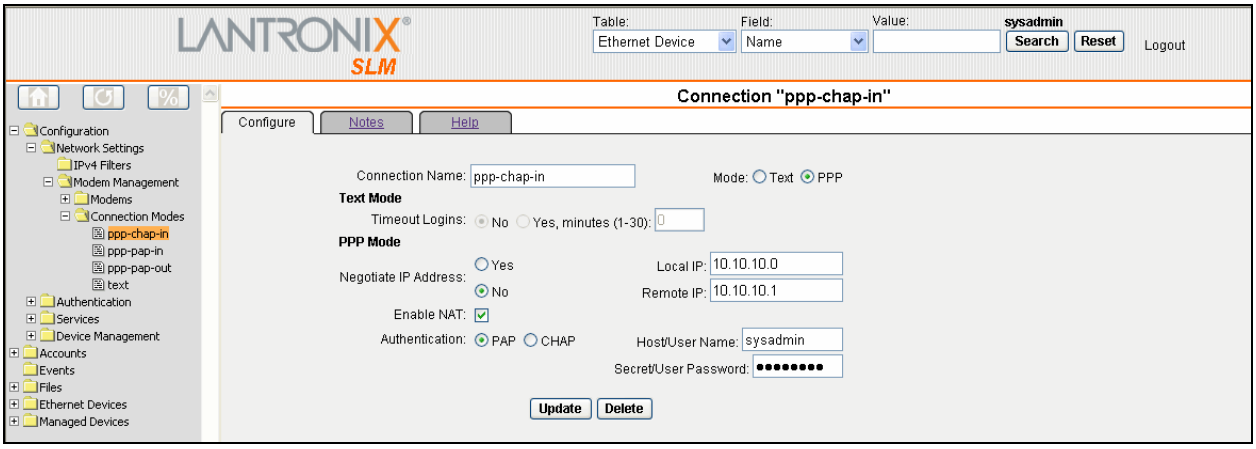
Updating and Deleting a Connection

The administrator can update or delete connections.

To update or delete an IPv4 filters:

1. On the menu, click **Configuration→Network Settings→Modem Management→Connection Modes**, and then click the **Edit** icon to the left of the modem you want to update or delete. The **Configure** tab displays.

Figure 6-22. Connection Page — Configure Tab



2. To delete a connection:
   a) Click the **Delete** button.
   b) In response to the request for confirmation, click **OK**.
   c) Click **Connection Modes** on the menu tree. The deleted connection is no longer on the menu tree or listed on the **List** tab.
3. To update a connection:
   a) Edit the information as desired.
   b) Click the **Update** button. A confirmation message displays.

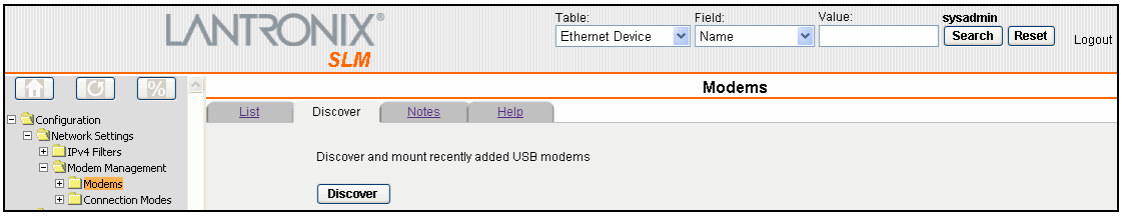
Note: *For information about configuring a dial-out connection, see* *Configuring a Modem Connection to a Managed Device on page 172.*

Discovering a USB Modem

The system administrator can attach a USB modem to an SLM and configure it into the system without rebooting the SLM.

To "discover" a USB Modem:

1. On the menu, click **Configuration→Network Settings→Modem Management→Modems** and then click the **Discover** tab. The Discover tab displays.



2. Click the **Discover** button. A message displays indicating that the task (discovering USB modems) has started.
3. After a few moments, refresh the tree structure. Any new USB modems display in the tree.

Modem Commands

reset modem connection

Note: You may only use this command when the modem is completely stuck.

Wait for minimum timeout period (3 minutes) before you use this command when:

- *You dial out via PPP and encounter no dial tone.*
- *You dial out via PPP and encounter a busy signal.*

Syntax

```
reset modem connection
```

Description

Resets a modem connection.

set modem disconnect

Note: Type `show modem` to view the current modem connections.

Syntax

```
set modem disconnect <Name>
```

Example

```
set modem disconnect MyPCIModem
```

Description

Terminates modem dial-out connection.

set modem edit

Syntax

```
set modem edit <Modem Name> <parameters>
```

Parameters

`name <New Name>`

`baud <300-115200>`

`flowcontrol <none|xon/xoff|rts/cts>`

`initscript <Modem Initialization Script>`

`defaultinitscript <Modem Default Initialization Script>`

`dialin <Dial Account Name|CLEAR|disable|enable>`

`CLEAR` removes the dial account assignment.

`disable` disables dial-in .

`enable` enables dial-in

`ipfilter <IPv4 Filter Name|CLEAR>`

`ipfilter CLEAR` removes the ipfilter assignment.

Description

Configures a currently loaded modem.

show modem

Syntax

`show modem`

Description

Displays all modems.

show modem connection

Syntax

show modem connection <parameters>

Parameters

`[index <number>]`

Description

Displays active (established) modem connections.

show modem settings

Syntax

`show modem <parameters>`

Parameters

`[name <Modem Name>]`

`[index <number>]`

Description

Displays modem settings.

show modem status

Syntax

`show modem status`

Description

Displays the status of the modem.

Dial Account Commands

set dialaccount add

Syntax

`set dialaccount add <Dial Account Name> <parameters>`

Parameters

`modemmode <`**`text`**`|ppp>`

Note: *If you select* `text`*, all other parameters except* `timeout` *are ignored.*

localipaddr <**negotiate**|IP Address>

remoteipaddr <**negotiate**|IP Address>

auth <**pap**|chap>

username <User Name>

password <Password>

nat <enable|**disable**>

Default is **20**.

Description

Creates a new dial account.

set dialaccount delete

Syntax

set dialaccount delete <Dial Account Name>

Description

Delete a dial account.

set dialaccount edit

Syntax

set dialaccount edit <Dial Account Name> <parameters>

Parameters

modemmode <text|ppp>

localipaddr <negotiate|IP Address>

remoteipaddr <negotiate|IP Address>

auth <pap|chap>

username <User Name>

password <Password>

nat <enable|disable>

forcedialback <disable|enable> (apply only text mode)

dialbacknumber <dial-back number|CLEAR> (apply only text mode)
CLEAR removes the dial-back number.

userprofile <disable|enable> (apply only text mode)
Uses local user-defined dial-back configuration.

timeout <disable|1-30 minutes>

Description

Modifies a dial account's settings.

set manageddevice config

Syntax

set manageddevice config <Device Name> [dialout <Dial Account Name|enable|disable> modem <Modem Name> phonenumber <phonenumber>]application <ssh|telnet|http|none>]

Description

Configures modem and dial account settings for a managed device.

set manageddevice index

Note: *Type* `show manageddevice all` *to display index.*

Syntax

```
set manageddevice index <number> [dialout <Dial Account
Name|enable|disable> modem <Modem Name> phonenumber
<phonenumber>]application ssh|telnet|http|none>]
```

Description

`Finds managed device by index and modifies dial account settings.`
To set modem parameters, you must specify a dial-out option.

set modem edit

Syntax

```
set modem edit <Modem Name> dialin <Dial Account
Name|CLEAR|disable|enable>
```

Description

Modifies a dial-in account name.

show dialaccount

Note: *Type* `show dialaccount` *to display index.*

Syntax

```
show dialaccount <parameters>
```

Parameters

```
[name <Dial Account Name>]
```

```
[index <number>]
```

Examples

```
show dialaccount
```

```
show dialaccount name ppp-pap
```

```
show dialaccount index 2
```

Description

Displays dial account settings.

show dialaccount mapping

Syntax

```
show dialaccount mapping
```

Description

Shows dial account used by dial-in and dial-out.

7: User Management

This chapter is primarily for administrators, who configure authentication methods, add, update, and delete accounts and account groups, and grant account and account group permissions.

By default, local authentication is enabled and is the first method the SLM uses to authenticate users. The administrator can select additional authentication methods, such as NIS, LDAP, RADIUS, SecurID, and SSH public key or CLI login. The ability to assign different degrees of access to individual users or user groups provides another level of security.

User Authentication Methods

On this page you may enable, disable and order methods for authenticating users attempting to log in to the SLM. The methods include NIS, LDAP, RADIUS, Kerberos, TACACS+, SecurID, and Local. The authentication method selection on the SLM does not affect devices or SLM interaction with devices.

By default, local authentication is enabled and is the first method the SLM uses to authenticate users. The ability to assign different degrees of access to individual users or user groups provides another level of security.

The authentication method selection on the SLM does not affect devices or SLM interaction with devices.

Note: *For a user to be authenticated using one of the remote methods, the user's account must be configured for remote access (**Remote Only** or **Local & Remote**), or there must be a account defined whose login name is the same as the protocol (e.g., "NIS" for NIS).*

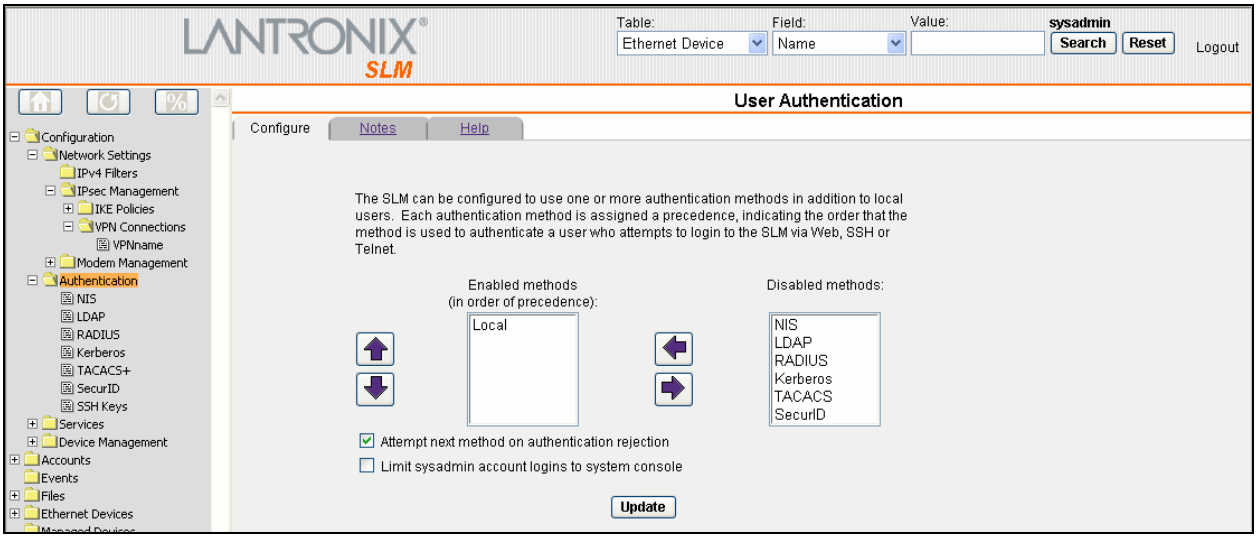
If you enable multiple authentication methods, the SLM attempts login authentication in the order specified. When **Attempt next method on authentication rejection** is enabled, login authentication continues until a configured method reports success or all configured methods have been exhausted. When **Attempt next method on authentication rejection** is disabled, login authentication continues until a configured method reports success or failure, skipping non-responding methods.

Note: *Adding an NIS user with the same user name as a local user may result in undefined behavior. For this reason, the SLM prevents the addition of such accounts when NIS is configured and enabled, but it is unable to stop the creation of such accounts when NIS is disabled. The other remote authentication types are not affected by this issue.*

To enable, disable, and set the precedence of authentication methods:

1. On the menu, click **Configuration→Authentication**. The following page opens:

Figure 7-1. User Authentication Page – Configure Tab



2. To enable a method currently in the **Disabled methods** list, select the method and click the **left arrow**.

   The methods include:

Local	The SLM authenticates users in the local database by user name and password. If this method is enabled, it always responds.
NIS (Network Information System)	A network naming and administration system developed by Sun Microsystems for smaller networks. Each host client or server computer in the system has knowledge about the entire system. A user at any host can access files or applications on any host in the network with a single user name and password. NIS uses the client/server model and the Remote Procedure Call (RPC) interface for communication between hosts. NIS consists of a server, a library of client programs, and some administrative tools. NIS is often used with the Network File System (NFS).
LDAP (Lightweight Directory Access Protocol)	A set of protocols for accessing information directories, specifically X.500-based directory services. LDAP runs over TCP/IP or other connection-oriented transfer services.

RADIUS (Remote Authentication Dial-In User Service)	An authentication and accounting system used by many Internet Service Providers (ISPs). It is a client/server protocol that enables remote access servers to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It increases security, allowing a company to set up a policy that can be applied at a single administered network point. Select RADIUS if a RADIUS server is used as a proxy for SecurID. Select SecurID if a native SecurID server is used.
Kerberos	Kerberos is a network authentication protocol that enables two parties to exchange private information across an unprotected network. It works by assigning a unique electronic credential, called a *ticket,* to each user who logs on to the network. The ticket is embedded in messages to identify the sender.
TACACS+ (Terminal Access Controller Access Control System)	TACACS+ allows a remote access server to communicate with an authentication server to determine whether the user has access to the network. TACACS+ is a completely new protocol and is not compatible with TACACS or XTACACS. The SLM supports TACACS+ only.
SecurID	SecurID is a two-factor authentication method based on the user's SecurID token and pin number. The SecurID token displays a string of digits called a token code that changes once a minute (some tokens are set to change codes every 30 seconds). Select RADIUS if a RADIUS server is used as a proxy for SecurID. Select SecurID if a native SecurID server is used.

3. To disable a method currently in the **Enabled methods** list, select the method and click the **right arrow** between the lists.
4. To set the order in which the SLM will authenticate users, click the **up** and **down arrows** to the left of the **Enabled methods** list.
5. To instruct the SLM to attempt authentication using the next configured method in the list when an authentication method responds to, and fails, a login, select the **Attempt next method on authentication rejection** check box.
6. Click the **Apply** button.

Now that you have enabled one or more authentication methods, you must configure them.

NIS

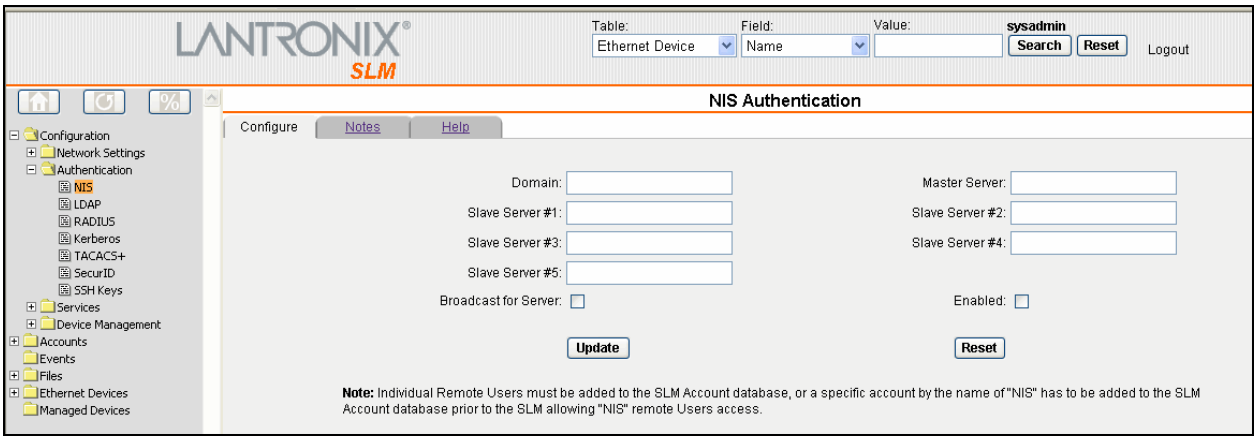
The administrator can configure the SLM to use NIS to authenticate users attempting to log in to the SLM through the web interface, SSH, Telnet, or the console port.

Note: *For a user to log in remotely using NIS, the user's account must have remote access (**Remote Only** or **Local & Remote**), or there must be an account defined whose login name is **NIS**. (See Accounts on page 109 for information on setting up accounts.)*

To configure the SLM to use NIS to authenticate users:

1. On the menu, click **Configuration→ Authentication→NIS**. The following page opens.

Figure 7-2. NIS Authentication Page – Configure Tab



2. Enter the following:

Domain	The NIS domain of the SLM must be the same as the NIS domain of the NIS server.
Master Server (required)	The IP address or hostname of the master server.
Broadcast for Server	Select the check box for the SLM to send a broadcast datagram to find the NIS Server on the local network.
Slave Server #1 - 5	The IP addresses or hostnames of up to five slave servers.
Enabled	Displays selected if you previously enabled this method on the User Authentication page or on this page. To configure this authentication method but not enable it, clear the check box. ***Note:*** *You can enable this authentication method here or on the User Authentication page. If you enable it here, it is assigned the lowest priority on the User Authentication page.*

3. To save, click the **Update** button. A confirmation message displays.

LDAP

The administrator can configure the SLM to use LDAP to authenticate users attempting to log in to the SLM through the web interface, SSH public key, Telnet, or the console port.

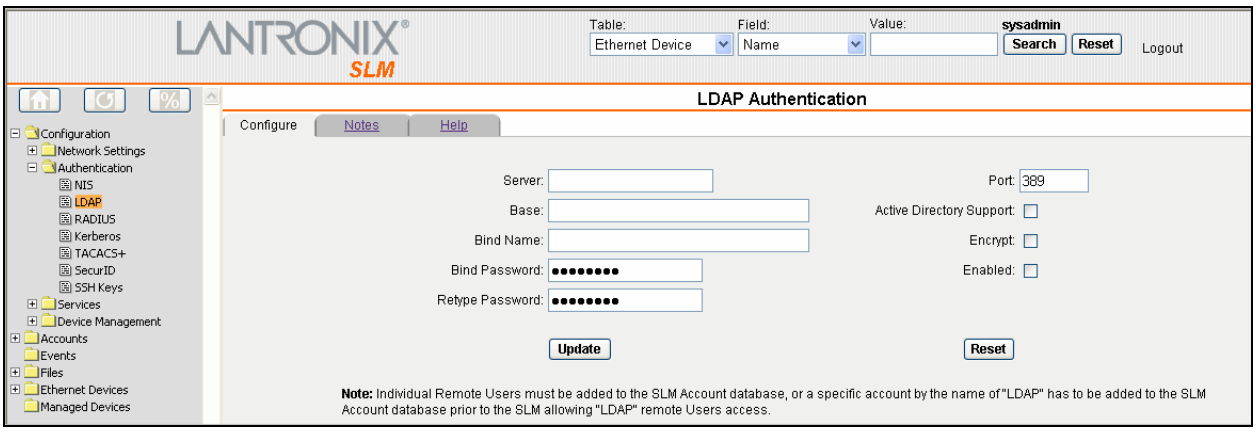
LDAP allows SLM users to authenticate using a wide variety of LDAP servers, such as OpenLDAP and Microsoft Active Directory. The LDAP implementation supports LDAP servers that do not allow anonymous queries.

Note: *For a user to log in remotely using LDAP, the user's account must have remote access (**Remote Only** or **Local & Remote**), or there must be an account defined whose login name is **LDAP**. (See Accounts on page 109 for information on setting up accounts.)*

To configure the SLM to use LDAP to authenticate users:

1. On the menu, click **Configuration→ Authentication→LDAP**. The following page opens.

Figure 7-3. LDAP Authentication Page – Configure Tab



2. Enter the following:

Server	The IP address or host name of the LDAP server.
Base	The name of the LDAP search base (e.g., dc=company, dc=com). May have up to 80 characters.
Bind Name	The name for a non-anonymous bind to an LDAP server. This item has the same format as LDAP Base. One example is cn=administrator,cn=Users,dc=domain,dc=com
Bind Password and **Retype Password**	Password for a non-anonymous bind. This entry is optional. Acceptable characters are **a-z**, **A-Z,** and **0-9**. The maximum length is 127 characters.
Port	Number of the TCP port on the LDAP server to which the SLM talks. The default setting is **389**.
Active Directory Support	Select to enable. Active Directory is a directory service from Microsoft that is a part of Windows 2000 and later versions of Windows. It stores information about network resources within a domain. It is LDAP- and Kerberos-compliant. Disabled by default.

Encrypt	Select to encrypt messages between the SLM and the LDAP server. Disabled by default.
Enabled	Displays selected if you previously enabled this method on the User Authentication page or on this page. To configure this authentication method but not enable it, clear the check box. ***Note:*** *You can enable this authentication method here or on the User Authentication page. If you enable it here, it is assigned the lowest priority on the User Authentication page.*

3. To save, click the **Update** button. A confirmation message displays.

RADIUS

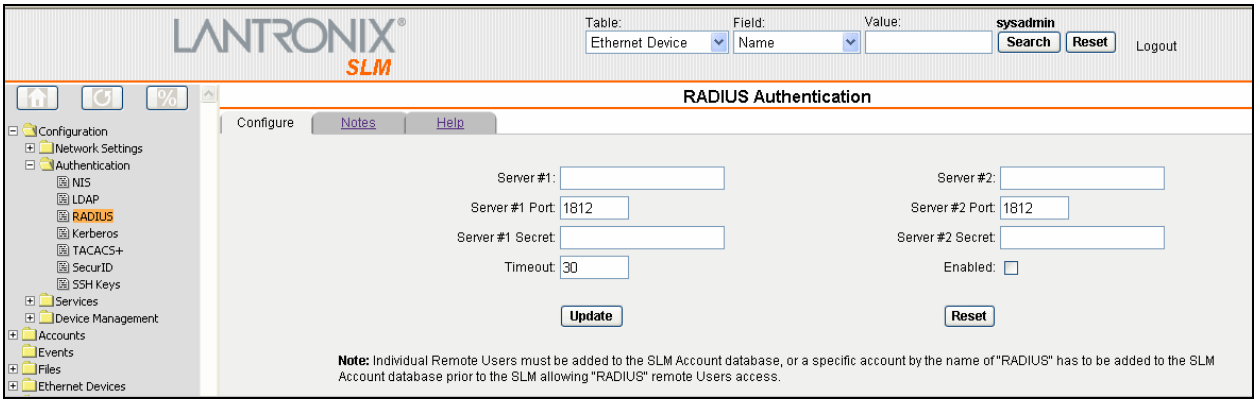
The administrator can configure the SLM to use RADIUS to authenticate users attempting to log in to the SLM through the web interface, SSH public key, Telnet, or the console port.

Note: *For a user to log in remotely using RADIUS, the user's account must have remote access (**Remote Only** or **Local & Remote**), or there must be an account defined whose login name is **RADIUS**. (See Accounts on page 109 for information on setting up accounts.)*

To configure the SLM to use RADIUS to authenticate users:

1. On the menu, click **Configuration→User Authentication→RADIUS**. The following page opens.

Figure 7-4. RADIUS Authentication Page – Configure Tab



2. Enter the following:

Server #1	IP address or hostname of the primary RADIUS server. This RADIUS server may be a proxy for SecurID. For native SecurID, use the SecurID configuration web page.

Server #1 Port	Number of the TCP port on the RADIUS server used for the RADIUS service. If you do not specify an optional port, the SLM uses the default RADIUS port (**1812**). ***Note:*** *Older RADIUS servers may use 1645 as the default port. Check your RADIUS server configuration.*
Server #1 Secret	Text that serves as a shared secret between a RADIUS client and the server (SLM). The shared secret is used to encrypt a password sent between the client and the server. May have up to 128 characters.
Server #2	IP address or hostname of the secondary RADIUS server.
Server #2 Port	Number of the TCP port on the RADIUS server used for the RADIUS service. If you do not specify an optional port, the SLM uses the default RADIUS port (**1812**). ***Note:*** *Older RADIUS servers may use 1645 as the default port. Check your RADIUS server configuration.*
Server #2 Secret	Text that serves as a shared secret between a RADIUS client and the server (SLM). The shared secret is used to encrypt a password sent between the client and the server. May have up to 128 characters.
Timeout	The number of seconds after which the connection attempt times out. The default setting is **30**.
Enabled	Displays selected if you previously enabled this method on the User Authentication page or on this page. To configure this authentication method but not enable it, clear the check box. ***Note:*** *You can enable this authentication method here or on the User Authentication page. If you enable it here, it is assigned the lowest priority on the User Authentication page.*

3. To save, click the **Update** button. When the update is complete, a confirmation message displays.

Kerberos

Kerberos is a network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography.

The administrator can configure the SLM to use Kerberos to authenticate users attempting to log in to the SLM through the web interface, SSH, Telnet, or the console port.

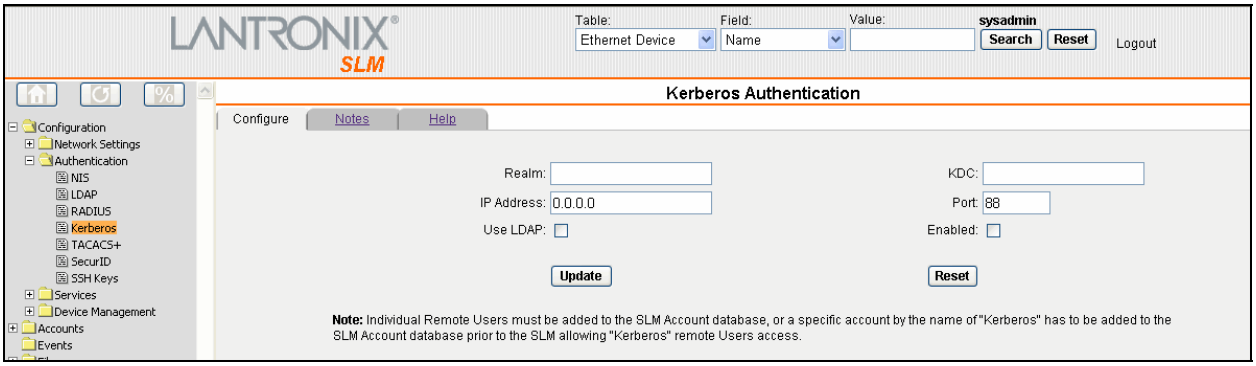
Note: *For a user to log in remotely using Kerberos, the user's account must have remote access (**Remote Only** or **Local & Remote**), or there must be an account defined whose*

*login name is **Kerberos**. (See Accounts on page 109 for information on setting up accounts.)*

To configure the SLM to use Kerberos to authenticate users:

1. On the menu, select **Configuration→ Authentication→ Kerberos**. The following page opens.

Figure 7-5. Kerberos Authentication Page – Configure Tab



2. Enter the following:

Realm	Enter the name of the logical network served by a single Kerberos database and a set of Key Distribution Centers. Usually, realm names are all uppercase letters to differentiate the realm from the Internet domain. Realm is similar in concept to an NT domain.
KDC	A key distribution center (KDC) is a server that issues Kerberos tickets. A ticket is a temporary set of electronic credentials that verify the identity of a client for a particular service. Enter the **KDC** in the fully qualified domain name format (FQDN). An example is SLC.local.
IP Address	Enter the IP address of the Key Distribution Center (KDC).
Port	Port on the KDC listening for requests. Enter an integer with a maximum value of 65535. The default setting is **88**.
Use LDAP	Indicate whether Kerberos should rely on LDAP to look up user IDs and Group IDs. This setting is disabled by default. ***Note:* Make sure to configure LDAP if you select this option.**
Enabled	Displays selected if you previously enabled this method on the User Authentication page or on this page. To configure this authentication method but not enable it, clear the check box. ***Note:** You can enable this authentication method here or on the User Authentication page. If you enable it here, it is assigned the lowest priority on the User Authentication page.*

3. To save, click the **Update** button. A confirmation message displays.

TACACS+

Similar to RADIUS, the main function of TACACS+ is to perform authentication for remote access. The SLM supports the TACACS+ protocol (not the older TACACS or XTACACS protocols).

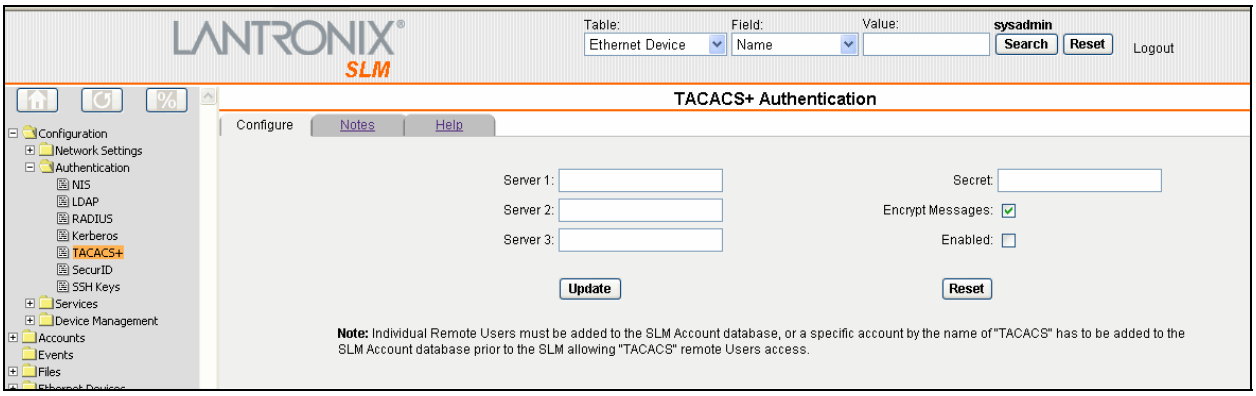
The administrator can configure the SLM to use TACACS+ to authenticate users attempting to log in to the SLM through the web interface, SSH, Telnet, or the console port.

Note: *For a user to log in remotely using TACACS+, the user's account must have remote access (**Remote Only** or **Local & Remote**), or there must be an account defined whose login name is **TACACS**.*

To configure the SLM to use TACACS+ to authenticate users:

1. On the menu, select **Configuration→Authentication→TACACS**. The following page opens.

Figure 7-6. TACACS+ Authentication Page – Configure Tab



2. Enter the following:

Servers 1-3	IP address or host name of up to three TACACS+ servers.
Secret	Shared secret for message encryption between the SLM and the TACACS+ server. Enter an alphanumeric secret of up to 127 characters.
Encrypt Messages	Select the check box to encrypt messages between the SLM and the TACACS+ server. Selected by default.
Enabled	Displays selected if you previously enabled this method on the User Authentication page or on this page. To configure this authentication method but not enable it, clear the check box. ***Note:*** *You can enable this authentication method here or on the User Authentication page. If you enable it here, it is assigned the lowest priority on the User Authentication page.*

3. To save, click the **Update** button. A confirmation message displays.

SecurID

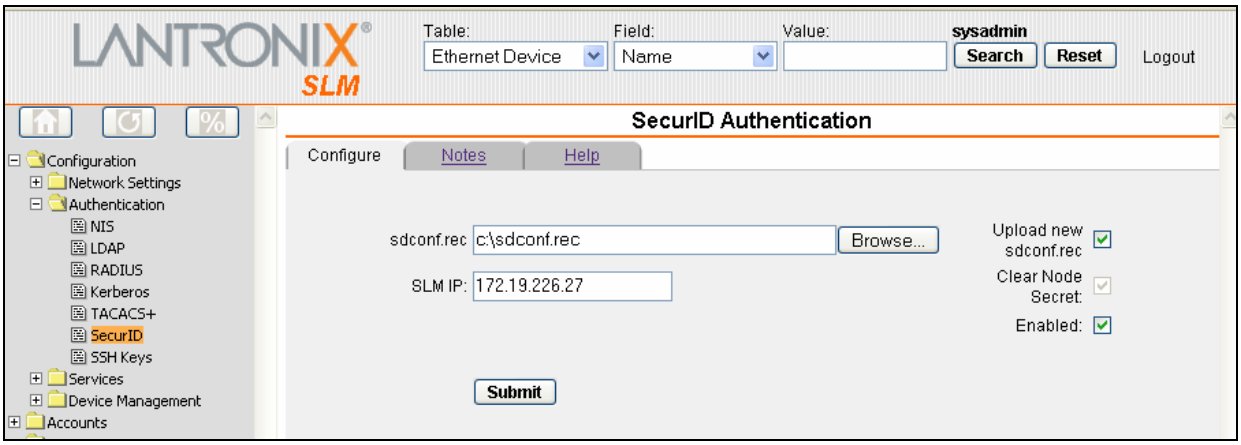
SecurID is a two-factor authentication method based on a SecurID token and a pin number. An analogous two-factor authentication method is an ATM card combined with a pin number. The SecurID token displays a string of digits called a token code that changes once a minute (some tokens are set to change codes every 30 seconds).

The administrator can configure the SLM to use SecurID to authenticate users attempting to log in to the SLM through the web interface, SSH, Telnet, or the console port. Selecting this option will disable all other authentication methods, as SecurID cannot be used in conjunction with other methods.

To configure the SLM to use SecurID to authenticate users:

1. On the menu, select **Configuration→Authentication→SecurID**. The following page opens.

Figure 7-7. SecurID Authentication Page



2. Enter the following information:

sdconf.rec/Upload new sdconf.rec	Configuration file generated by the SecurID server. To upload this file from the Administrator's browser client, select the **Upload new sdconf.rec** checkbox and select the file with the **Browse** button.
SLM IP	The SLM's IP address as configured on the SecurID server. The SecurID server uses this to validate the identity of the SLM.
Clear Node Secret	Upon the first successful authentication, the SecurID server places a shared node secret key on the SLM. There may be times when this file needs to be cleared by both sides, so this option is available.
Enabled	Select the checkbox to enable SecurID authentication. You can also select this option on the User Authentication page. **Selecting this option will disable all other authentication methods, as SecurID cannot be used in conjunction with other methods.** The local sysadmin account will still be able to log in, but can be limited to system console logins if desired on the User Authentication page.

3. To save, click the **Submit** button.

SSH Keys

The SLM can import and export SSH keys to facilitate shared key authentication for all incoming and outgoing SSH connections. By using a public/private key pair, a user can access multiple hosts with a single passphrase, or, if a passphrase is not used, a user can access multiple hosts without entering a password.

For imported and exported SSH keys, the SLM supports both RSA and DSA keys and can import and export keys in OpenSSH and SECSH formats. Both imported and exported keys must be associated with a local SLM user.

Imported Keys

Imported SSH keys must be associated with an SLM local user. The key can be generated on host "MyHost" for user "MyUser," and when the key is imported into the SLM, it must be associated with either "MyUser" (if "MyUser" is an existing SLM local user) or an alternate SLM local user. The public key file can be imported through SCP or FTP; once the file is imported, you can view or delete the public key. Any SSH connection into the SLM from the designated host/user combination uses the SSH key for authentication.

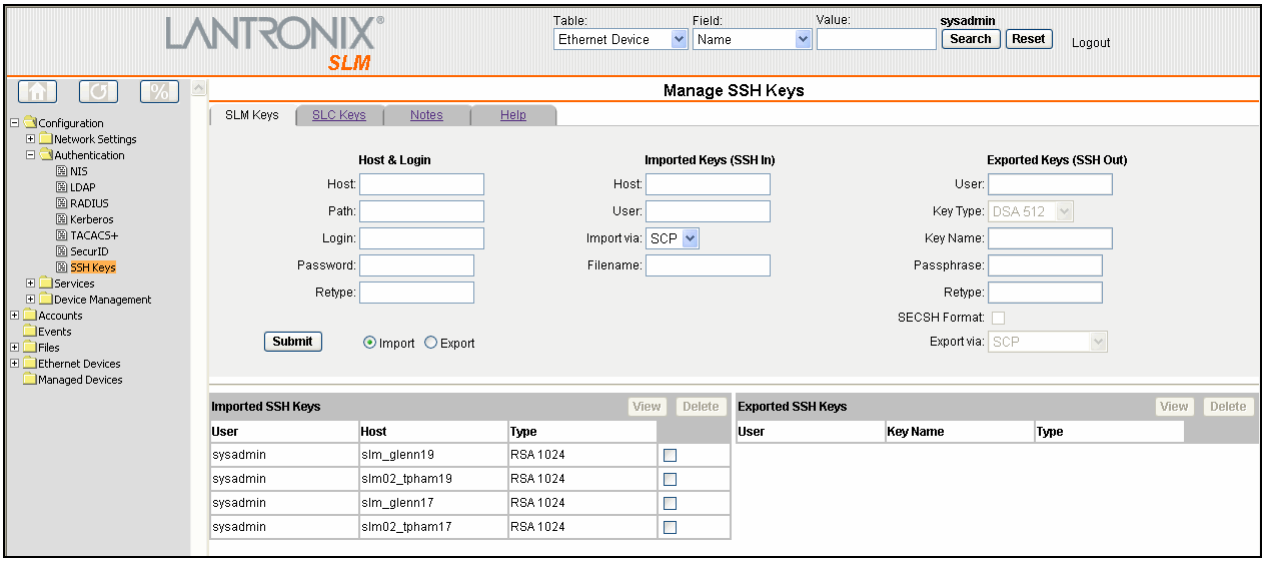
Exported Keys

The SLM can generate SSH keys for SSH connections out of the SLM for any SLM user. The SLM retains both the private and public key on the SLM, and makes the public key available for export through SCP, FTP, or copy and paste. The name of the key is used to generate the name of the public key file that is exported (for example, <keyname>.pub), and the exported keys are organized by user and key name. Once a key is generated and exported, any SSH connection out of the SLM for the designated host/user combination uses the SSH key for authentication.

To configure the SLM to use SSH keys to authenticate users:

1. On the menu, select **Configuration→Authentication→SSH Keys**. The following page opens.

Figure 7-8. Manage SSH Keys – SLM Keys Tab



2. To the right of the **Submit** button, click **Import** or **Export** to indicate the type of keys you are setting up.
3. Enter the following:

Host and Login

Host and Login

Host	IP address of the remote server from which to SCP or FTP the public key file.
Path	Optional pathname to the public key file.
Login	User ID to use to SCP or FTP the file.
Password/Retype	Password to use to SCP or FTP the file.

Imported Keys (SSH In)

These entries (the **Host, User, Import via**, and **Filename** fields are always required for importing keys) are required in the following cases:

- The imported key file does not contain the host from which the user will be making an SSH connection.
- The SLM local user login for the connection is different from the user name from which the key was generated or is not included in the imported key file.

If either of these conditions is true, or the imported file is in SECSH format, you must specify the host and user. The following is an example of a public key file that includes the host and user:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAEEApUHCX9EWsHt+jmUGXa1YC3us
ABYxIXUhSU1N+NU9HNaUADUFfd8LYz8/gUnUSH4Ksm8GRT7/8/Sn9jCVfGPh
UQ== asallaway@winserver
```

Host	Host name or IP address from which the SSH connections to the SLM will be made.
User	User ID of the person given secure access to the remote server.
Import via	Select **SCP** or **FTP** as the method for importing the SSH keys. The default is **SCP**.
Filename	Name of the public key file (for example, mykey.pub).

Exported Keys (SSH Out)

User	User ID of the person given secure access to the remote server.
Key Type	Select either the **RSA** or the **DSA** encryption standard followed by the number of bits (**512** or **1024**) in the key. **DSA 512** is the default. All export fields are disabled during import and vice versa.
Key Name	Name of the key. This will generate the public key filename (e.g., <keyname>.pub).
Passphrase/Retype	Optionally, enter a passphrase associated with the key. The passphrase may have up to 50 characters. The passphrase is an optional password that can be associated with an SSH key. It is unique to each user and to each key.

SECSH Format	Indicate whether the keys will be exported in **SECSH** format. The default is **OpenSSH**.
Export via	Select the method (**SCP**, **FTP**, or **Cut and Paste)** of exporting the key to the remote server. **Cut and Paste**, the default, requires no other parameters for export.

4. Click the **Submit** button. The keys display in the list below.
5. To view a user's key, select the user and click the **View** button.
6. To delete a user's key, select the user and click the **Delete** button.

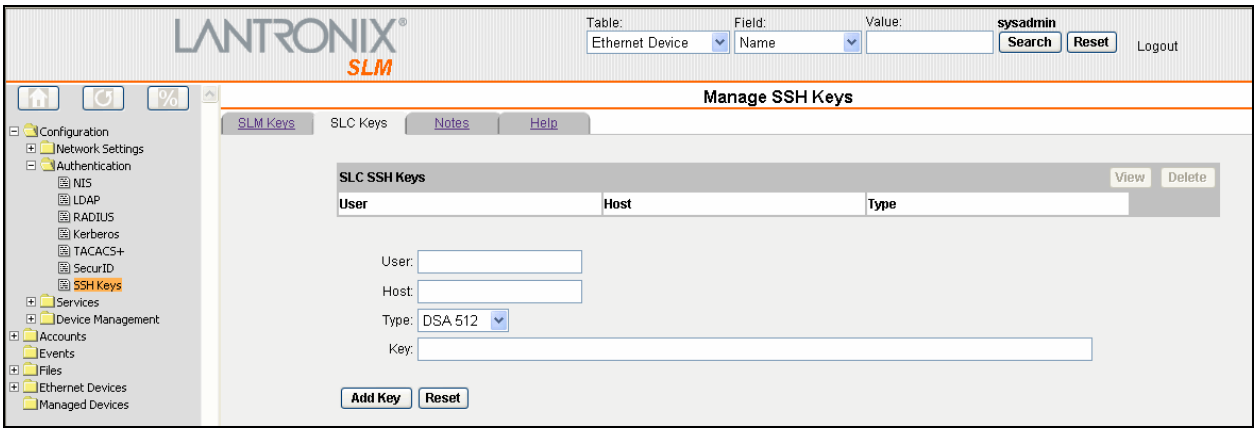
To add or view export SLC keys:

You can enable the SLM to retrieve all the public keys (each with a specific user and host name) from a particular SLC and store them in the SLM database. Then you can push those public keys to other SLCs, allowing those particular users to access the other SLCs from those particular hosts.

Note: *For information about importing and exporting keys, see* *Using the Actions Tab on page 217,*

1. On the menu, select **Configuration→Authentication→SSH Keys**, and click the **SLC Keys** tab. The following page opens:

Figure 7-9. Manage SSH Keys – SLC Keys Tab



2. Enter the following information:

User	User login of the person given secure access to the SLC.
Host	Host name or IP address from which the SSH connections to the SLC will be made.
Type	Select either the **RSA** or the **DSA** encryption standard followed by the number of bits (**512** or **1024**) in the key. **DSA 512** is the default. All export fields are disabled during import and vice versa.
Key	Enter the SSH key content.

3. Click the **Add Key** button. The key information (except the key itself) displays in the table on the top of the page.
4. To view the key, select the check box for the user, and click the **View** button in the top right of the page. The SLC key displays.

Example of an SLC key:

SLC key for sysadmin@SLM_tpham17

RSA 1024:
AAAAB3NzaC1yc2EAAAABIwAAAQEAvy7zXy+l1YDbaXalMYVRKGPBue+HdR+ih
mdZZqGcN8xcO2Lqdwb6lyJO4QN4PcQ6n88VwLM0/UEJgW1PF3vp/Z+kKw4v48
NHJUOZSKRfTejMssgp1S6TTf+YWzHCr1mX/+yRUyA+I9VXb9cI2r9uqIlMk/GVTg
pl/8YERnAsQ9AeRfy/20MXOSGg895tdBW6piLKWoJ5P6NRcXsFJScmowGXNU4
snUpk2cvVNyGiVMe9jb454fb080+/lphmMrJMUPYX3uG22Qsm0KZGosnLFKtYzim
DaOoRQ2QI9my19i/baFX9RiH2yda+vLmBsTchaEx30Dp7PwbaHi7gf8Rb9Q==

5. To delete one or more keys:
   a) Select the check box for each key to be deleted and click the **Delete** button.
   b) In response to the request for confirmation, click **OK.**

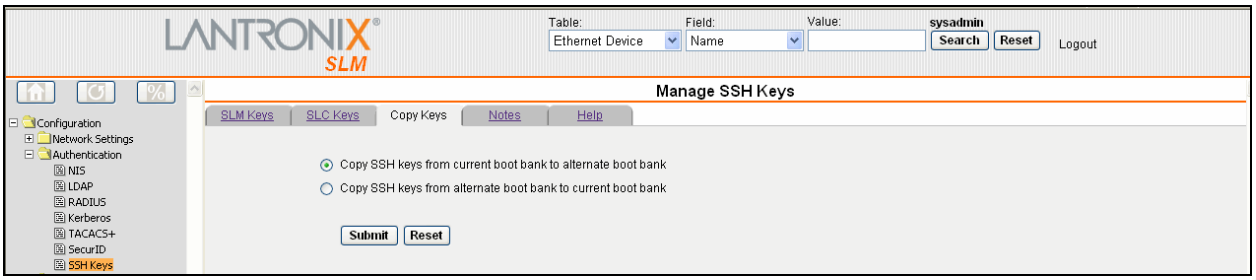
Copy Keys

If your SLM is set up with dual booting, you can move SSH keys from one boot partition to another.

To copy a key:

1. On the menu, select **Configuration > Authentication > SSH Keys**, and then click the **Copy Keys** tab.

Figure 7-10. Manage SSH Keys – Copy Keys Tab



2. **Select one of the following:**
   - **Copy SSH keys from current boot bank to alternate boot bank.**
   - **Copy SSH keys from alternate boot bank to current boot bank.**
3. Click the **Submit** button.
4. To return to the original settings, click the **Reset** button.

Authentication Commands

set auth

Syntax

```
set auth <one or more parameters>
```

Parameters

```
local <1-7>
nis <1-7>
```

```
ldap <1-7>
radius <1-7>kerberos <1-7>
tacacs+ <1-7>
securid <1-7>
authusenextmethod <enable|disable>
limitsysadmin <enable|disable>
```

Description

Sets ordering of authentication methods and how authentication methods are used.

Authentication can occur using all methods, in the order of their precedence, until a successful authentication is obtained, or using only the first authentication method that responds (in the event that a server is down).

Note: *If SecurID is used, no other parameters can be used.*

Any methods omitted from the `set auth` command will be disabled if at least one method is selected

set ldap

Syntax

```
set ldap <one or more parameters>
```

Parameters

```
state <enable|disable>
server <IP Address or Name>
 port <TCP Port>
 base <LDAP Base>
 bindname <Bind Name>
 bindpassword <Bind Password>
 adsupport <enable|disable>
 encrypt <enable|disable>
```

Description

Configures the SLM to use LDAP to authenticate users who log in to the SLM via SSH, Telnet, the web, or the console port.

set nis

Syntax

```
set nis <one or more parameters>
```

Parameters

```
<enable|disable>
 domain <NIS Domain Name>
 broadcast <enable|disable>
 master <IP Address or Name>
 slave1 <IP Address or Name>
```

```
slave2 <IP Address or Name>
slave3 <IP Address or Name>
slave4 <IP Address or Name>
slave5 <IP Address or Name>
```

Description

Configures the SLM to use NIS to authenticate users who log in to the SLM via SSH, Telnet, the web, or the console port.

set radius

Syntax

```
set radius <one or more parameters>
state <enable|disable>
timeout <1-30 seconds>
server1 <IP Address or Name>
port1 <TCP Port>
secret1 <Secret>
server2 <IP Address or Name>
port2 <TCP Port>
secret2 <Secret>
```

Description

Configures the SLM to use RADIUS to authenticate users who login to the SLM via SSH, Telnet, the web, or the console port.

set sshkey delete

Syntax

```
set sshkey delete keyuser <SSH Key User> keyhost <SSH Key Host>
```

Description

```
Deletes an imported SSH key.
```

set sshkey import

Syntax

```
set sshkey import <copypaste>
```

Note: *RSA keys must be 1024 bits*

Description

Imports an SSH key.

show auth

Syntax

```
show auth
```

Description

Displays authentication methods in use.

show ldap

Syntax

```
show ldap
```

Description

Displays all LDAP information.

show nis

Syntax

```
show nis
```

Description

Displays all NIS information.

show radius

Syntax

show radius

Description

Displays all RADIUS information.

show sshkey import

Syntax

```
show sshkey import <one or more parameters>
```

Parameters

```
[keyuser <SSH Key User>]
[keyhost <SSH Key IP Address or Name>]
[viewkey <enable|disable>]
```

Description

Displays imported SSH keys.

Account Groups

The administrator organizes accounts into account groups to simplify the task of assigning permissions. Accounts inherit device rights from the account group to which they belong. To assign unique permissions to an individual account, it must be the only member of an account group. The **sysadmin** account always has all permissions enabled.

Note: *Only functions and devices for which the user has rights display in that user's menu on the web interface or on the CLI.*

Account Group Types

There are four types of account groups: Administrators, Ethernet Device, Managed Device, and Menu Only.

Administrators Account Group: Has rights and permissions to configure the SLM and to add, edit, and delete account groups within the Ethernet Device, Managed Device, and Menu Only categories. Administrators cannot delete or rename the Administrators Group, although they can add additional accounts to it. Administrators have access to configuration, events, logs, and files, can create groups of managed devices, and interact with Ethernet and managed devices. Administrators can log into both the web interface and the CLI.

Ethernet Device Account Groups: Can interact with SLCs, SLKs, SLPs, and other SLMs, other Lantronix devices, some non-Lantronix device, the ports of the devices, and the managed devices created from these ports to which the group has rights. Ethernet Device Account groups can log into both the web interface and the CLI. Ethernet Device Account groups may also create, update, and delete Managed Device Groups and assign managed devices to which they have rights (by having rights to their parent Ethernet device) to those groups.

Managed Device Account Groups: Have access to the managed devices (e.g., servers and switches) connected to Ethernet device ports to which the group has rights. Managed Device Account Groups can log into both the web interface and the CLI.

Menu Only Account Groups: These groups can log into the CLI but not the web interface. They can interact with managed devices only. The administrator assigns a restricted menu of numbered options that these users can select.

Viewing Account Groups

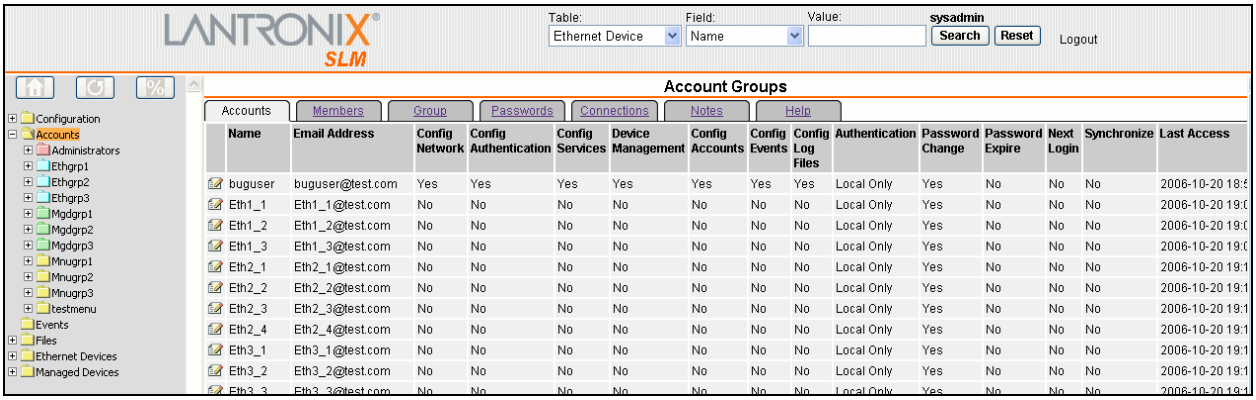
Administrators can view account groups.

To view account groups:

1. On the menu, click **Accounts.**

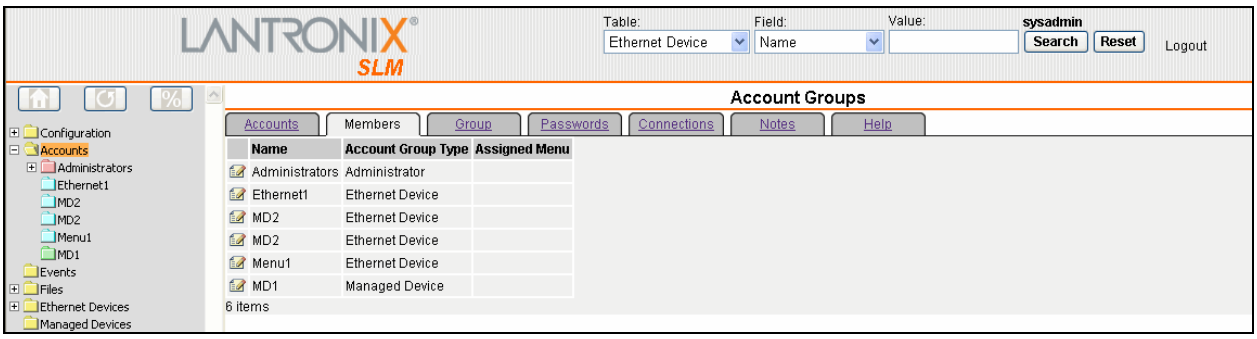
   The following page opens:

Figure 7-11. Account Groups Page – Accounts Tab


LANTRONIX SLM
Table: Ethernet Device
Field: Name
Value:
sysadmin
Search
Reset
Logout
Account Groups
Accounts
Members
Group
Passwords
Connections
Notes
Help
Configuration
Accounts
Administrators
Ethgrp1
Ethgrp2
Ethgrp3
Mgdgrp1
Mgdgrp2
Mgdgrp3
Mnugrp1
Mnugrp2
Mnugrp3
testmenu
Events
Files
Ethernet Devices
Managed Devices
Name
Email Address
Config Network
Config Authentication
Config Services
Device Management
Config Accounts
Config Events
Config Log Files
Authentication
Password Change
Password Expire
Next Login
Synchronize
Last Access
buguser buguser@test.com Yes Yes Yes Yes Yes Yes Yes Local Only Yes No No No 2006-10-20 18:
Eth1_1 Eth1_1@test.com No No No No No No No Local Only Yes No No No 2006-10-20 19:
Eth1_2 Eth1_2@test.com No No No No No No No Local Only Yes No No No 2006-10-20 19:
Eth1_3 Eth1_3@test.com No No No No No No No Local Only Yes No No No 2006-10-20 19:
Eth2_1 Eth2_1@test.com No No No No No No No Local Only Yes No No No 2006-10-20 19:1
Eth2_2 Eth2_2@test.com No No No No No No No Local Only Yes No No No 2006-10-20 19:1
Eth2_3 Eth2_3@test.com No No No No No No No Local Only Yes No No No 2006-10-20 19:1
Eth2_4 Eth2_4@test.com No No No No No No No Local Only Yes No No No 2006-10-20 19:1
Eth3_1 Eth3_1@test.com No No No No No No No Local Only Yes No No No 2006-10-20 19:1
Eth3_2 Eth3_2@test.com No No No No No No No Local Only Yes No No No 2006-10-20 19:1

2. Click the **Members** tab. A list of existing account groups displays.

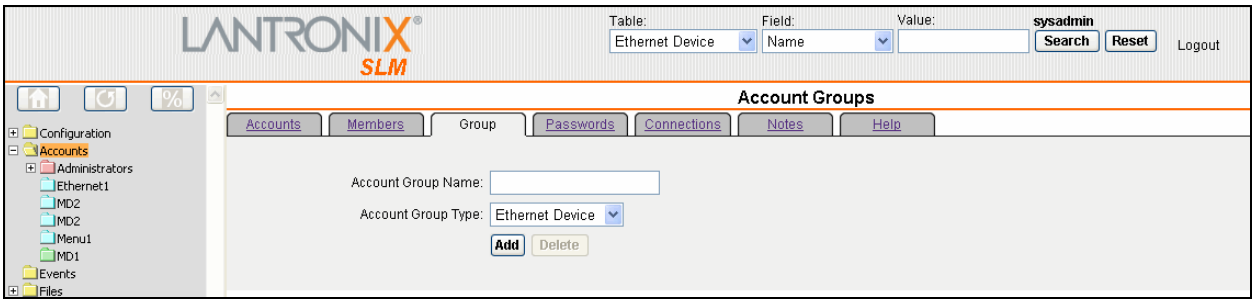
Figure 7-12. Account Groups Page – Members Tab



Adding an Account Group

1. On the Account Groups page, click the **Group** tab. The following page opens:

Figure 7-13. Account Group Page – Group Tab



2. Enter the following:

Account Group Name	The name of the new account group.
Account Group Type	From the drop-down list, select the type of account group. The default setting is **Ethernet Device**.

3. To save, click the **Add** button. A confirmation message displays and the new group displays in the **Accounts** menu tree.
4. To display the list of account groups, click **Accounts** on the menu. The new group is on the list.

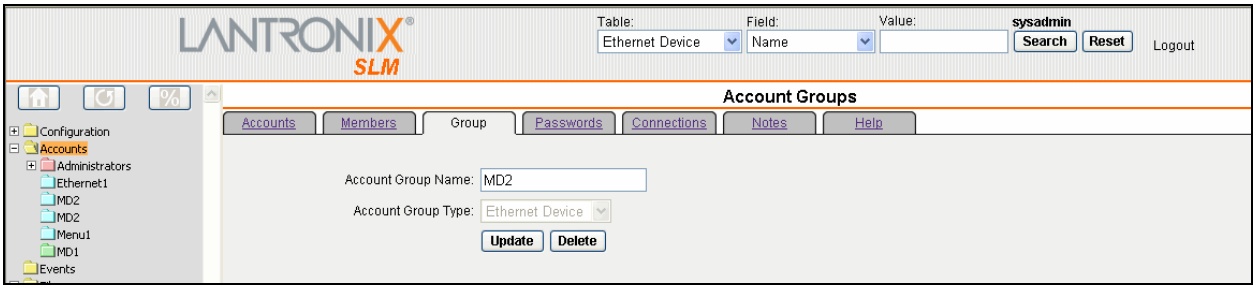
Updating or Deleting an Account Group

The administrator can update or delete any group except for **sysadmin**.

To update or delete an account group:

1. On the **Accounts** tab, click the **Edit** icon to the left of the group you want to update or delete. The **Group** tab displays.

Figure 7-14. Account Groups – Group Tab



2. To delete an account group:

   Note: You can rename an *account group but not change its type. You cannot delete an account group if it contains any accounts; delete the accounts first.*

   a) Click the **Delete** button.

   b) In response to the request for confirmation, click **OK**. A blank **Group** tab opens.

   c) Click **Accounts** on the menu tree. The deleted group is no longer on the menu tree or listed on the **Members** tab.

3. To update the name of an account group:

   a) Edit the name as desired.

   b) Click the **Update** icon. A confirmation message displays.

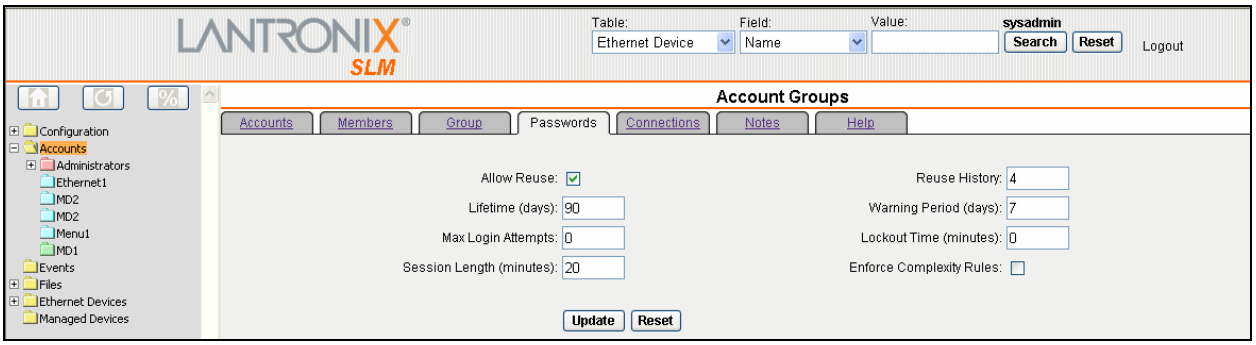
   c) Click **Accounts** on the menu tree. The updated group is on the menu tree and listed on the **Members** tab.

Setting Password Requirements for Account Groups

The administrator sets parameters for passwords that apply to all accounts.

1. On the Account Groups page, click the **Passwords** tab.

Figure 7-15. Account Groups Page – Passwords Tab.



2. Enter the following information:

Allow Reuse	Select to enable users to continue to reuse old passwords. If you disable the check box, the user cannot use any of the **Reuse History** number of passwords. Enabled by default.
Reuse History	The number of passwords the user must use before reusing an old password. The default is 4. For example, if you set reuse history to 4, the user may reuse an old password after using 4 other passwords.
Lifetime (days)	The number of days until the password expires. The default setting is **90**.
Warning Period (days)	The number of days ahead that the system warns that the user's password will expire. The default setting is **7**.
Max Login Attempts	The number of times the user can attempt to log in unsuccessfully before the system locks the user out. The default setting is **0** (disabled).
Lockout Time (minutes)	The number of minutes the locked-out user must wait before trying to log in to the web interface again. The default setting is **0** (disabled).
Session Length (minutes)	The number of minutes a session can be idle before it times out. The minimum is five minutes. The default setting is **20**. This applies to both web and CLI sessions. ***Note:*** *The SLM ships with a default maximum of 25 concurrent user sessions (or "seats"). If you require more than 25 concurrent user sessions, please contact your sales associate to order them. When all seats are in use, the sysadmin can still log in one more time, from the CLI interface only, and terminate other connections.*
Enforce Complexity Rules	Select to enable the SLM to enforce rules concerning the password structure (e.g., alphanumeric requirements, number of characters, punctuation marks). Disabled by default. **Complexity rules:** ◆ Passwords must be at least eight characters long. ◆ Passwords must contain one upper case letter (A-Z), one lower case letter (a-z), one digit (0-9), and one punctuation character ((\)`~!@#$%%^&*-+=\{}[]:;"'<>,.?/_).

3. To save, click the **Update** button. When the update is complete, a confirmation message displays.

Assigning Account Group Device Rights

Accounts inherit the device rights of the account group to which they belong. Administrators can add or remove permission to an account group to view, configure, or interact with specific Ethernet devices or specific ports and the managed devices connected to them.

Administrators Account Group: Can view, configure, and interact with all Ethernet devices and with the managed devices connected to the Ethernet device's ports.

Ethernet Device Account Groups: Can view, configure, and interact with specific Ethernet devices, their ports, and the managed devices connected to the ports.

Managed Device Account Groups: Can view, configure, and interact with specific managed devices.

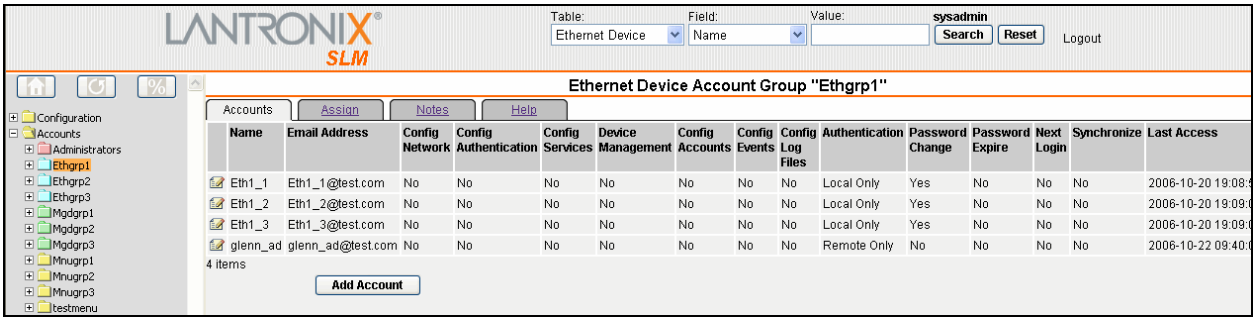
Menu Only Account Groups: Can view and interact with specific managed devices, according to the menu they have permission to use.

To assign permissions to an Ethernet Device Account Group:

The administrator assigns permissions to an Ethernet Device Account Group to access specific Ethernet devices. All members of the group inherit these permissions.

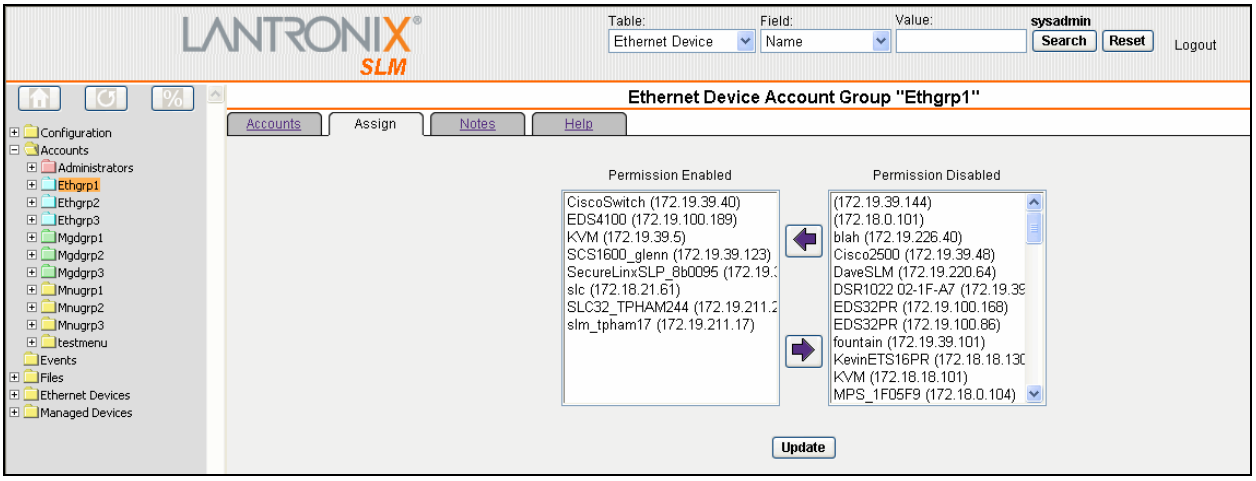
1. Select the account group from the menu. The following page opens.

Figure 7-16. Ethernet Device Account Group – Accounts Tab



2. Click the **Assign** tab. The following page opens:

Figure 7-17. Ethernet Device Account Group – Assign Tab



This tab displays two lists: **Permission Enabled** and **Permission Disabled**.

Note: *You can use* ***Ctrl+click*** *to select multiple devices from these lists.*

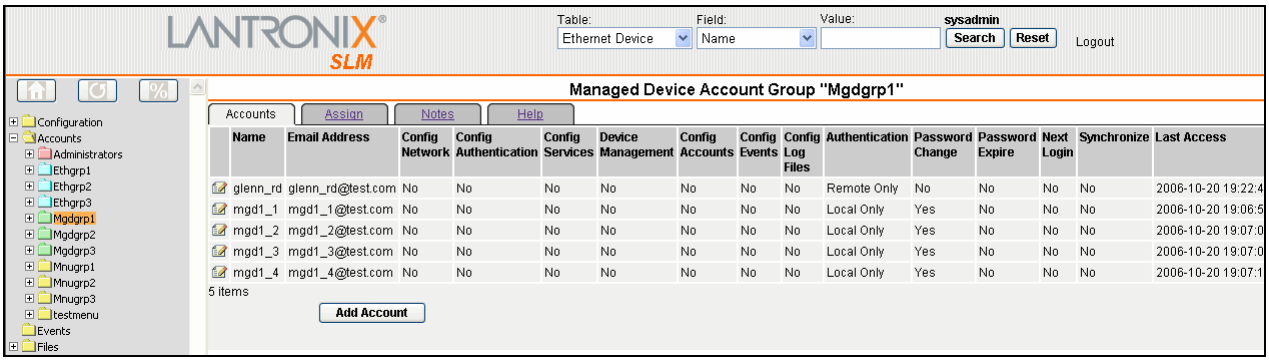
3. To enable access to a device listed in **Permission Denied**, select the device and click the **left arrow**. The device is now in the **Permission Enabled** list.
4. To remove access to a device, select the device in the **Permission Enabled** list and click the **right arrow**. The device is now in the **Permission Disabled** list.
5. Click the **Update** button. When the update is complete, a confirmation message displays. When the user logs in, only Ethernet and managed devices for which the user has permission display in the menu tree.

To assign permissions to a Managed Device Account Group:

The administrator assigns permissions that allow a Managed Device Account Group to access specific managed devices. All members of the group inherit these permissions.

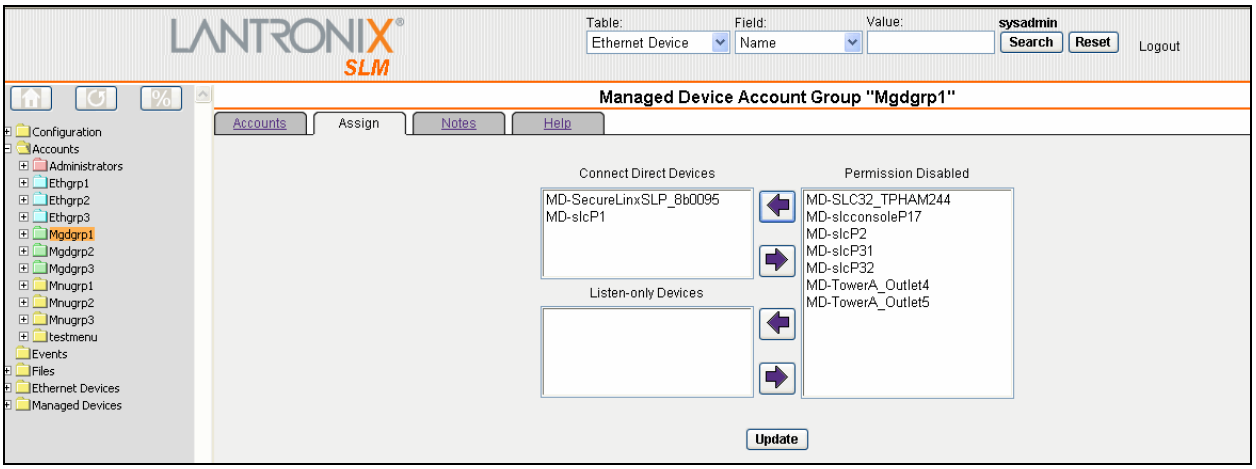
1. Select the account group from the menu. The following page opens:

Figure 7-18. Managed Device Account Group – Accounts Tab



2. Click the **Assign** tab.

Figure 7-19. Managed Device Account Group – Assign Tab



3. To enable permission to read from and write to a managed device connected to an Ethernet device port, select it from the **Permission Disabled** list and click the top **left arrow**. The device displays in the **Connect Direct Devices** list.

Note: *You can use* **Ctrl+Right click** to select multiple devices.

4. To enable permission to listen only to a managed device, select it from the **Permission Disabled** list and click the bottom **left arrow**. The device displays in the **Listen-only Devices** list.
5. To disable permission for a managed device, select it from the **Connect Direct Devices** or **Listen-only Devices** list, and click the corresponding **right arrow**. The device displays in the **Permission Disabled** list.
6. Click the **Update** button. When the update is complete, a confirmation message displays. When the user logs in, only managed devices for which the user has permission display on the menu tree.

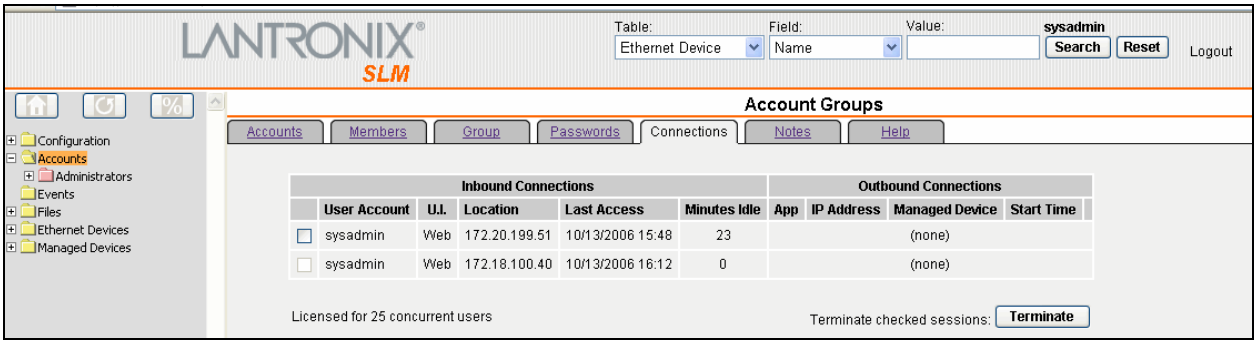
Viewing Currently Logged-In Accounts

Administrators can see which users are currently logged into the SLM and whether they are connected to any managed devices. The page also displays the maximum number of concurrent users for which this SLM is licensed.

To view logged-in accounts:

1. On the menu, click **Accounts,** and then click the **Connections** tab. The following page opens:

Figure 7-20. Account Groups – Connections Tab



2. View the following information:

Inbound Connections:

User Account	User name for logging in to the SLM.
U.I.	Type of interface (web or command line) the user is logged in to.
Location	IP address of the client.
Last Access	Date and time the user last accessed the SLM.
Minutes Idle	Number of minutes since the user last took an action in the session.

Outbound Connections

App	Application used to manage the device.
IP Address	IP address of the managed device.

Managed Device	Name of the managed device.
Start Time	Time the SLM made the connection.

3. To terminate a session, select the check box for the inbound or outbound session(s) and click the **Terminate** button.

   Note: *All outbound connections associated with a closed inbound session will also close.*

4. To refresh the page only, click the **Terminate** button with no sessions selected.

Account Group Commands

set accountgroup add

Syntax

```
set accountgroup add <Group Name> type <ethernet|managed|menu>
<parameters>
```

Parameters

```
[menu <Menu Name>]
```

Description

Creates a local account group. Group type is Administrators, Ethernet, Managed, or Menu User.

set accountgroup edit

Syntax

```
set accountgroup edit <Group Name> <one or more parameters>
```

Parameters

```
[name <new name>]
```

```
[menu <Menu Name|CLEAR>]
```

Description

Modifies an account group. Group type is Administrators, Ethernet User, Managed User, or Menu User. `CLEAR` removes the current menu assignment.

show accountgroup

Syntax

```
show accountgroup <Group Name>
show accountgroup name <Group Name>
```

Description

Displays account group information.

show accountgroup all

Syntax

```
show accountgroup all
```

```
show accountgroup
```

Description

Displays information about all account groups.

show accountgroup index

Note: *Type* `show accountgroup all` *to display the index.*

Syntax

```
show accountgroup index <number>
```

Description

Displays account groups by index number.

Accounts

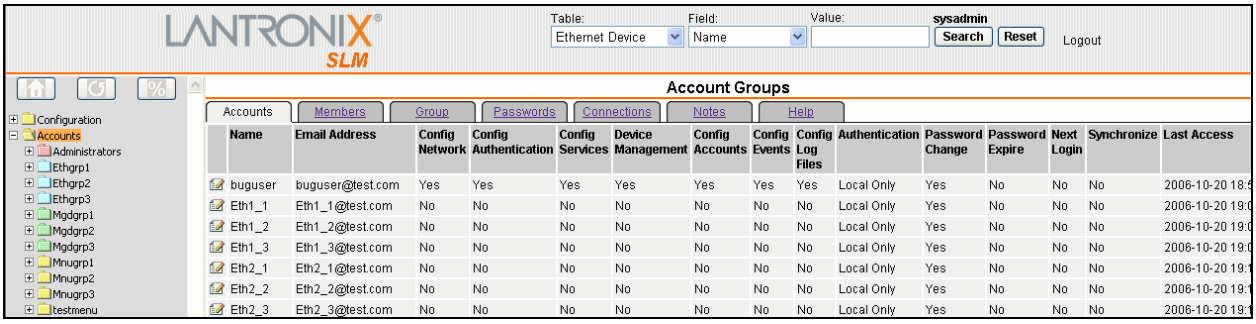
The Accounts page is for administrators who add, update, and delete accounts. Accounts inherit device rights from the account group to which they belong. To assign unique permissions to an individual account, create the account as the sole member of an account group. The **sysadmin** account always has all permissions enabled.

Note: *Only functions and devices for which the user has rights display in that user's menu on the web interface or on the CLI.*

Viewing Accounts

1. On the menu, click **Accounts**. The **Accounts** tab on the Account Groups page displays a list of authenticated users with the functions each user has permission to perform.

Figure 7-21. Account Groups -- Accounts Tab



2. View the following information about each user:

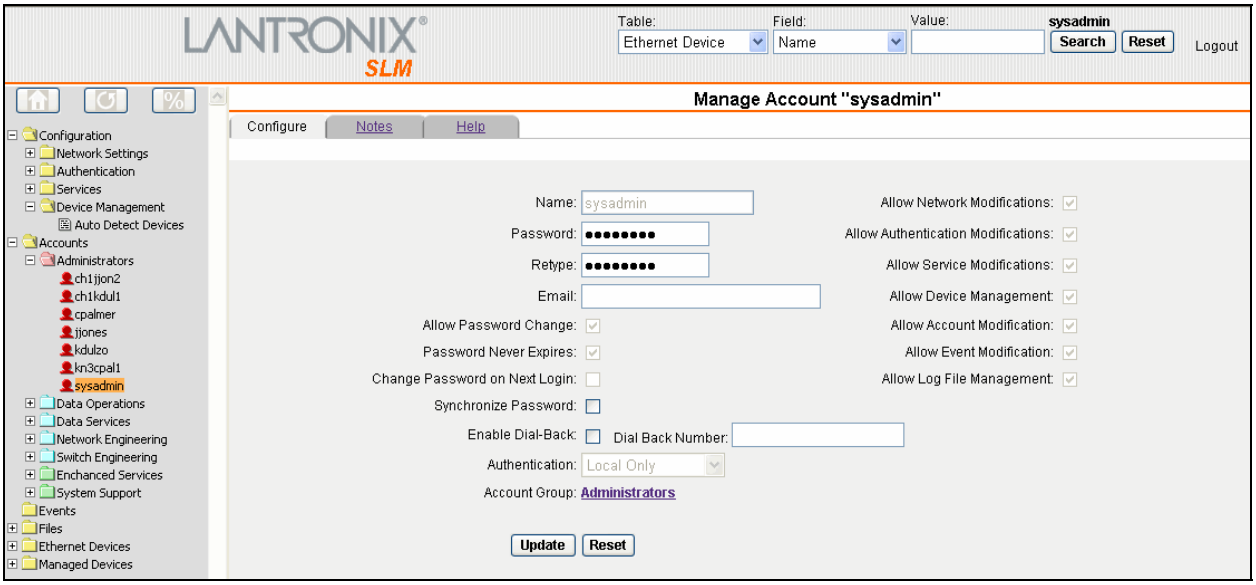
Note: *Only Administrator accounts may have the configuration flags enabled.*

Name	The user name for logging in to the SLM.
Email Address	User's email address; may be used for event notification.
Config Network	Indicates whether the user has permission to open the Network Settings page and configure network settings.

Config Authentication	Indicates whether the user has permission to select and prioritize authentication methods and to configure related settings.
Config Services	Indicates whether the user has permission to configure services such as date and time and SNMP Agent & syslog and to update SLCs to which the user has access.
Device Management	Indicates whether the user has permission to configure settings for auto-detecting devices and ports and for managing alternate SLMs.
Config Accounts	Indicates whether the user has permission to add, update, and delete all accounts and to grant account permissions.
Config Events	Indicates whether the user has permission to set alarms and triggers.
Config Log Files	Indicates whether the user has permission to view, copy, and delete various log files.
Authentication	Indicates whether authentication for this user is **Local Only**, **Remote Only**, **Local & Remote**, or **Disabled**.
Password Change	Indicates whether the user has permission to use the current password indefinitely.
Password Expire	**No** allows the user to keep a password indefinitely.
Change Password Next Login	Indicates whether the user has permission to change the password the next login.
Synchronize	When the Push Passwords check box on the Maintenance page is selected, the SLM uses the password on all accounts with **Synchronize Password** enabled to update accounts on remote SLMs, SLCs, SCSxx05/20s, and SLPs. The accounts must have access rights to and local user accounts on the devices. ***Notes:*** *SLP password synchronization uses SSH and CLI commands not an SNMP command, so you must provide the sysadmin login and password in the SLP device page for SLP password synchronization to work.* *Rebooting the SLM for any reason causes it to ignore user account password changes made but not yet pushed before the reboot.*
Last Access	Date and time the account group was last updated.

3. Click the **Edit** icon to the left of a user. The following page opens:

Figure 7-22. Account Page – Configure Tab



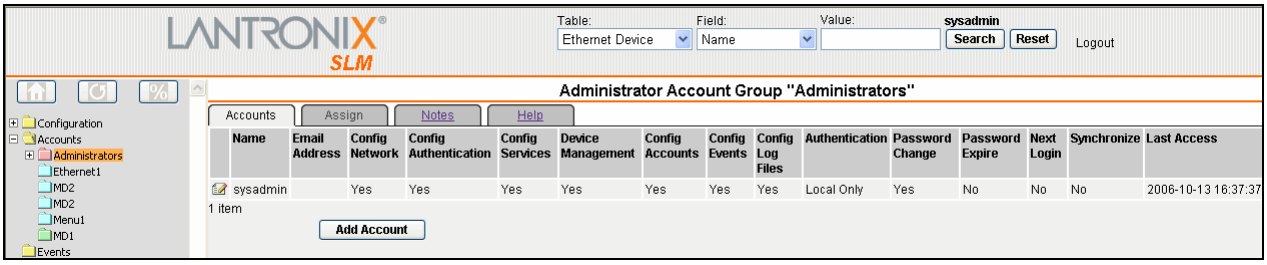
Adding an Account to the Administrators Account Group

The sysadmin account can add other administrators to the Administrators Group, assigning a user name and email address for each user. The name is for logging in over the web interface or the command line interface. The SLM uses the email address to send emails to users based on configured alarm settings.

To add a user to the Administrators Group:

1. On the menu, click **Accounts→Administrators Group**. The following page opens:

Figure 7-23. Administrator Account Group – Accounts Tab



2. Click the **Add Account** button at the bottom of the table. The following page opens:

Figure 7-24. Add New Account to Group – Configure Tab

3. Enter the following information:

User Name and Password

Name	User ID for logging into the SLM. Must be alphanumeric, start with an alpha character, and may include an underscore (_).
Password and Retype	User's password for logging in to the SLM.
Email	User's email address.
Allow Password Change	Select to allow user to change passwords. Enabled by default.
Password Never Expires	Selected by default. Select to allow the user to use current password indefinitely. Selected by default.
Change Password on Next Login	Select to require the user to change the password the next time the user logs in. (You may change this setting at any time.)
Synchronize Password	When the **Push Passwords** check box on the Maintenance page is selected, the SLM uses the password on all accounts with **Synchronize Password** enabled to update accounts on remote SLMs, SLCs, SCSxx05/20s, and SLPs. The accounts must have access rights to and local user accounts on the devices. ***Notes:*** *SLP password synchronization uses SSH and CLI commands not an SNMP command, so you must provide the sysadmin login and password on the SLP device page for SLP password synchronization to work.* *Rebooting the SLM for any reason causes it to ignore user account password changes made but not yet pushed.*

Enable Dial-Back	Users with dial-back access can dial into the SLM and enter their login and password. Once the SLC authenticates them, the modem hangs up and dials them back.
Dial Back Number	Select the phone number the modem dials back on. It can be a fixed number or a number associated with their login. If you select **Fixed Number**, enter the number (in the format 2123456789).
Authentication	From the drop-down list, select how the user will be authenticated **(Local Only**, **Remote Only,** or **Local & Remote**). The default setting is **Local Only**.
Account Group (link)	Click the link to view the Administrator Account group.

Permissions

Allow Network Modifications	Select to allow the user to configure network settings.
Allow Authentication Modifications	Select to allow the user to configure authentication settings.
Allow Service Modifications	Select to allow the user to configure settings for services.
Allow Device Management	Select to allow the user to auto-detect and to auto-save a configuration to another SLM.
Allow Account Modification	Select to allow the user to set up accounts and account groups.
Allow Event Modification	Select to allow the user to modify event settings.
Allow Log File Management	Select to allow the user to manage log files.

4. To save, click the **Add** button. A confirmation message displays, and the account displays in the **Administrators Group** on the menu tree.
5. Click **Administrators** on the menu tree. The Account Group **Accounts** tab opens. The added user displays in the list.

Adding an Account to an Ethernet or Managed Device Account Group

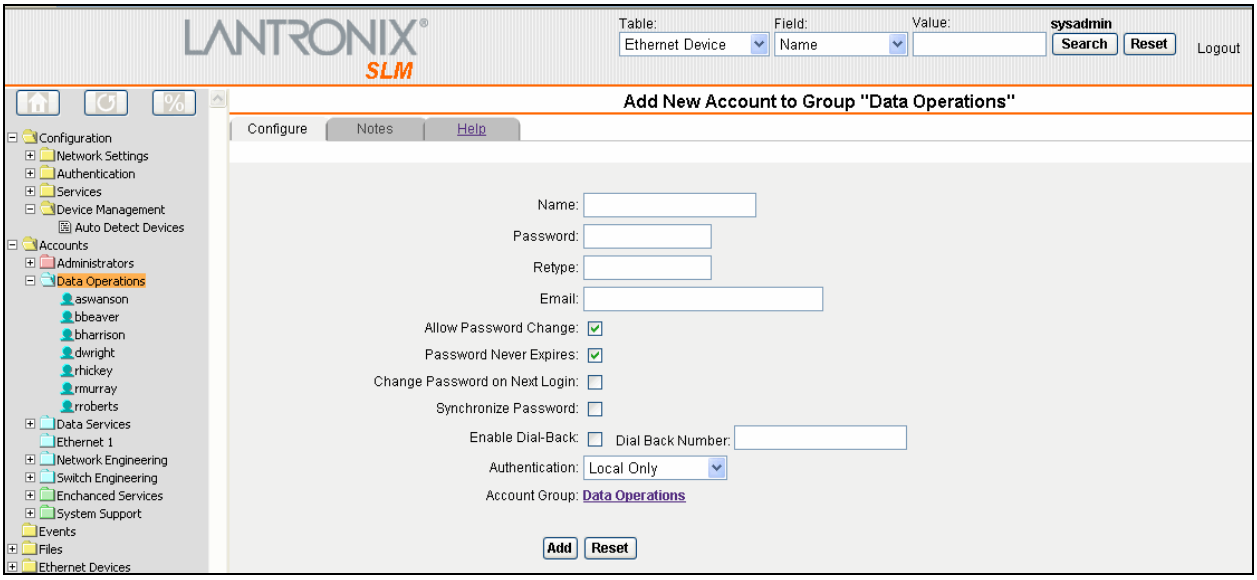
Administrators assign a user name and email address for each user. The name is for logging in over the web interface or the command line interface. The SLM uses the email address to send emails to users based on configured alarm settings.

To add an account to an Ethernet Device, Managed Device, or Menu Only Account Group:

Note: *In this section, we use the example of an Ethernet account.*

1. On the menu, select the account group.
2. Click the **Add Account button** at the bottom of the table. The following page opens:

Figure 7-25. Add New Accounts to Group – Configure Tab



3. Enter the following:

Name	User ID for logging into the SLM. Must be alphanumeric, start with an alpha, and may include an underscore (_).
Password and Retype	User's password for logging in to the SLM.
Email	User's email address.
Allow Password Change	Select to allow the user to change passwords. Selected by default.
Password Never Expires	Select to allow the user to use the current password indefinitely. Disabled by default.
Change Password on Next Login	Select to require the user to change the password the next time the user logs in. (You may change this setting at any time.)

Synchronize Password	When the **Push Passwords** check box on the Maintenance page is selected, the SLM uses the password on all accounts with **Synchronize Password** enabled to update accounts on remote SLMs, SLCs, SCSxx05/20s, and SLPs. The accounts must have access rights to and local user accounts on the devices. ***Notes:*** *SLP password synchronization uses SSH and CLI commands not an SNMP command, so you must provide the sysadmin login and password in the SLP device page for SLP password synchronization to work.* *Rebooting the SLM for any reason causes it to ignore user account password changes made but not yet pushed.*
Enable Dial-Back	Once the SLM authenticates them, users with dial-back access can dial into the SLM and enter their login and password. Once the SLC authenticates them, the modem hangs up and dials them back.
Dial Back Number	Select the phone number the modem dials back on. It can be a fixed number or a number associated with their login. If you select **Fixed Number**, enter the number (in the format 2123456789).
Authentication	From the drop-down list, select how the user will be authenticated (**Local Only**, **Remote Only**, or **Local & Remote**). The default setting is **Local Only**.
Account Group (link)	Click the link to view the parent Account Group page.

4. To save, click the **Add** button. A confirmation message displays.
5. Click the account group name on the menu tree. The account displays in the list of accounts and in the list on the **Accounts** tab.

Updating or Deleting an Account

Administrators can edit the password, email information, and configuration permissions for an account and remove accounts from an account group (except for the **sysadmin** account from the Administrators Group).

Note: *In this section, we use the example of an Ethernet account.*

To update an account or remove it from an account group:

1. In the menu tree, click the account. The following page opens:

Figure 7-26. Manage Account – Configure Tab

2. To update the account:
   a) Make changes as desired.
   b) Click the **Update** button.
3. To remove the account from the account group:
   a) Click the **Delete** button.
   b) In response to the confirmation request, click **OK**. A message confirming the deletion displays.
   c) To verify the deletion, click the account group in the menu. The user is no longer listed.

Account Commands

Use the following commands to configure local accounts (including **sysadmin**) to authenticate users who login to the SLM by means of SSH, Telnet, the web, or the console port.

`set account add`

Syntax

```
set account add <User Name> group <Group Name|admin>> <parameters>
```

Parameters

[email <Email Address>]

[auth <local|remote|localremote|disable>]

```
[allowdialback <enable|disable>]
[dialbacknumber <dial-back number>]
[allowpwchange <enable|disable>]
[pwneverexpires <enable|disable>]
[changepwnextlogin <enable|disable>]
```

Description

Creates a new user account.

set account delete

Syntax

```
set account delete <User Name>
```

Description

Deletes a user account.

set account edit

Syntax

```
set account edit <User Name> group <Group Name|admin> <parameters>
```

Parameters

```
[email <Email Address|CLEAR>]

Email CLEAR removes the current email.

[auth <local|remote|localremote|disable>

[allowdialback <enable|disable>]

[dialbacknumber <dial-back number|CLEAR>]

[allowpwchange <enable|disable>]

[pwneverexpires <enable|disable>]

[changepwnextlogin <enable|disable>]
```

Description

Modifies a user account.

set account password

Syntax

```
set account password <User Name>
```

Note: *Administrators with permission to change passwords must enter the username. Other users may not enter a username (they are changing their own password).*

Description

Configures a user account's password for the SLM.

show account

Syntax

```
show account <User Name>

show account user <User Name>
```

Description

Displays account information by user name.

show account all

Syntax

```
show account all
show account
```

Description

Displays all account names and information.

show account index

Note: *Type* `show account all` *to display the index.*

Syntax

```
show account index <number>
```

Description

Displays accounts by index number.

show account search

Syntax

Note: *All searches are case insensitive.*

```
show account search name <name>
show account search email <email address>
```

Examples

```
show account search name sys
```

Description

Searches for accounts by name or email address.

8: Ethernet Device Management

The SLM device database contains information about SLCs and other SecureLinx devices (SLKs, SLPs, and other SLMs) connected on the network. It may also contain information about other Lantronix and even non-Lantronix devices on the network, but you may have limited ability to manage them.

Administrators can enter SecureLinx management devices one at a time or, preferably, let the SLM auto-detect them. The SLM uses the Lantronix discovery protocol to auto-detect SecureLinx and other Lantronix devices, Lantronix SCS05/20 discovery protocol to auto-detect Lantronix SCS05/20 devices within a specified IP range, and SNMP to detect all other devices within a specified IP range.

Auto-Detecting Devices

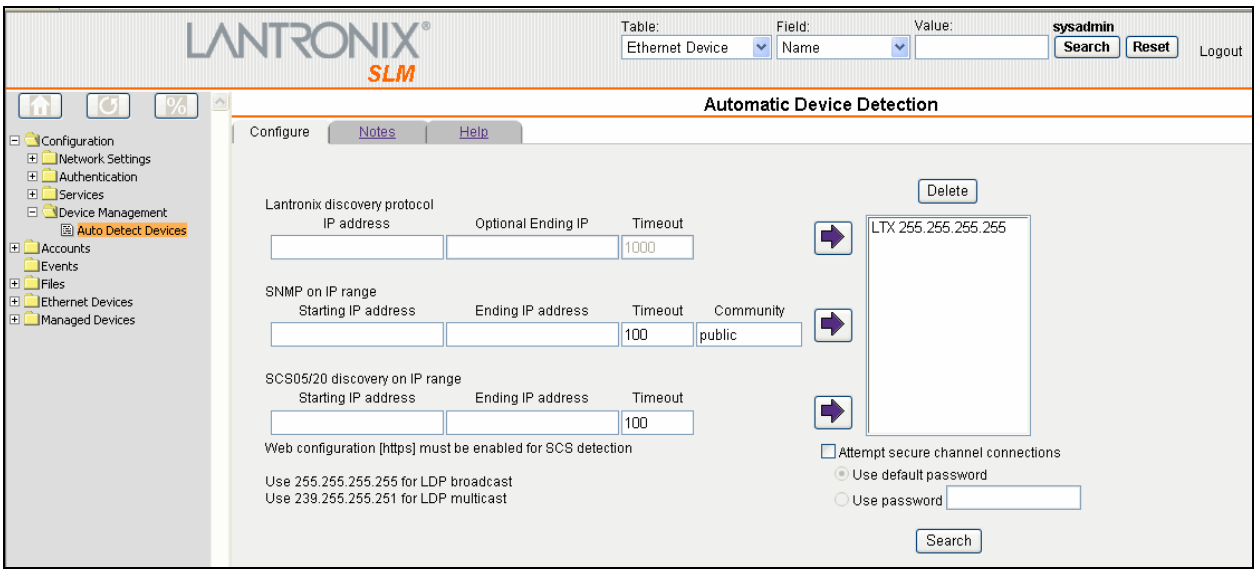
Auto-detect enables the SLM to search for and register Ethernet devices automatically. When the SLM detects an Ethernet device, it also scans the device for ports and port information. You only need to define search protocols and parameters once; they are saved for use in any future searches. When the SLM performs a device search, it uses all defined protocols simultaneously.

After performing an auto-detect search once, you need to run it again only if the search protocols change, or if new (undetected) devices are added to the network.

To auto-detect devices:

1. On the menu, click **Configuration→Device Management→Auto-Detect Devices**. The following page opens.

Figure 8-1. Automatic Device Detection Page – Configure Tab



2. *Enter the following information:*

Notes:

The maximum range of IP addresses to enter is 64K entries. We strongly recommend that you break the intended discovery range into several smaller ranges, to speed up the discovery process.

The discovery process may take up to 17 hours (1 second timeout for each entry) to complete for a full range of 64K IP entries; there is no option to cancel during discovery process.

Lantronix discovery protocol	This protocol discovers SLCs and other Lantronix-built devices on the network. ***Notes:*** ◆ Web configuration must be enabled on an SCS device for the SLM to discover it. ◆ To discover SLPs and SLKs, use SNMP; to discover SCSs, use SCS05/20 discovery. ◆ Use IP address **255.255.255.255** to discover all Lantronix-built devices on the local subnet, and use a remote subnet broadcast address if the routers in the network forward subnet broadcast packets. The Lantronix IP multicast address is **239.255.255.251.** Any device can join the 239.255.255.251 multicast group by notifying or registering to its subnet router. SLM then sends out a single discovery request, which is delivered to all devices in that multicast group by routers on different subnets. Once SLM gets a discovery response from members, it queries each individual device for further information. **Note:** See [RFC1112] for a description of the basic IGMP protocol. **IP address:** Specify the subnet (e.g., 255.255.255.255) to be searched, or if specifying a range of IP addresses, the IP address at the beginning of the range in which the SLM is to detect devices. **Optional Ending IP:** If specifying a range of addresses, enter the IP address at the end of the range. **Timeout:** Number of milliseconds the SLM will continue to look for a device before moving on. The default is **100**. ***Note:*** *You may specify more than one protocol search definition before the search.*

SNMP on IP range	Simple Network Management Protocol (SNMP) is a set of protocols for managing complex networks. Enter the following to discover all devices within one or more ranges of IP addresses on the network. SNMP requires that you specify a range of IP addresses. **Starting IP Address:** The IP address at the beginning of the range in which the SLM is to detect devices. **Ending IP Address:** The IP address at the end of the range in which the SLM is to detect devices. **Timeout:** Number of milliseconds the SLM will continue to look for a device before moving on. The default is **100**. **Community:** An SNMP community is the group to which devices and management stations running SNMP belong. The default setting is **public.**
SCS05/20 discovery on IP range	To locate Lantronix SCS05/20 products on the network, specify: **Starting IP Address:** The IP address at the beginning of the range in which the SLM is to detect devices. **Ending IP Address:** The IP address at the end of the range in which the SLM is to detect devices. **Timeout:** Number of milliseconds the SLM will continue to look for a device before moving on. The default is **100**. ***Note:*** *Web configuration must be enabled on an SCS device for the SLM to discover it.*
Attempt secure channel with default password	To establish a secure channel connection to discovered SLC and SLM devices, select the check box and one of the following options: **Use default password:** If you select this option, the SLM attempts to set up a secure channel to discovered SLCs and SLMs using the default sysadmin password of **PASS**. This is the default option. **Use password:** Enter a password to use for secure channel connections to discovered SLCs and SLMs. If the password has been changed, the user must manually establish secure channels on the device pages (using the appropriate password) later.

3. To add an entry to the current search list, click the **right arrow**.
4. To remove an entry from the current search list, select the entry and click the **Delete** button.
5. After defining all the searches, click the **Search** button.
6. If desired, check the progress of the search by clicking the progress button above the menu. The table shows how far along the search is towards completion.

   Note: *You can continue working while the auto-detect process takes place in the background.*

7. To add the detected devices to the menu tree, click the **Reload** button. When you open the device groups, the devices display in the proper place on the menu tree.

Note: *When you first auto-detect devices, all devices that respond are entered into the SLM database. You may decide to change the names of these devices (and ports) to something more meaningful than "SLC" or "Port-1." If you then auto-detect again, and auto-detect notices these devices again, the SLM retains the names you assigned. If you want to rename a device back to its original name, change the device name to ? before running the auto-detect. If auto-detect finds a device with the name ?, the SLM updates the name to the value the device returns.*

Auto-Detect Commands

admin autodetect filter delete

Syntax

```
admin autodetect filter delete
```

The command displays an index of current filters. Type the index number of the filter you want to delete and press **Enter**.

Description

Deletes one of the current auto-detect search filters.

admin autodetect filter ltrx

Syntax

```
admin autodetect filter ltrx <IP range> [timeout <number of
milliseconds>]
```

Example

```
IP range: 192.168.0.1-192.168.0.155 timeout 1500
timeout: default is 1000 ms; range is 1000-60000 ms
```

Description

Sets Lantronix discovery protocol search filters. The ending IP address is optional.

admin autodetect filter scs

Syntax

```
admin autodetect filter scs <IP range> [timeout <number of
milliseconds>]
```

Example

```
IP range: 192.168.0.1-192.168.0.155
timeout: default is 100 msec; range is 100-60000 msec
```

Description

Sets SCS discovery protocol search filters.

admin autodetect filter show

Displays the current auto-detect search filters.

Syntax

```
admin autodetect filter show
```

Description

Displays the current auto-detect search filters.

admin autodetect filter snmp

Syntax

```
admin autodetect filter snmp <IP range> [community <name>]
[timeout <number of milliseconds>]
```

Example

```
IP range: 92.168.0.1-192.168.0.155
name: public (default)
timeout:default is 100 msec; range is 100-60000 msec
```

Description

Sets SNMP protocol search filters.

admin autodetect start

Syntax

```
admin autodetect start <one or more parameters>
```

Parameters

`[securechannel <default|password>]`

`[option <ltrxonly|delnonltrx>}`

`ltrxonly` detects only Lantronix devices

`delnonltrx` detects only Lantronix devices and removes existing non-Lantronix devices.

Examples

`admin autodetect start securechannel default`
Attempts secure channel using the default password

`admin autodetect start securechannel mypass option delnonltrx`
Attempts secure channel using password `mypass`. Detects only Lantronix devices and removes existing non-Lantronix devices.

Description

Starts the SLM auto-detect device process, using the protocol and filters configured.

show progress

Syntax

```
show progress
```

Description

Shows the progress of background tasks.

Ethernet Devices

The SLM enables you to list all devices, groups of devices, and individual devices in the SLM database. These devices have been auto-detected or added manually. This section shows how the Administrator and Ethernet Device Account groups add devices manually, edit device settings, and delete devices.

Listing Devices

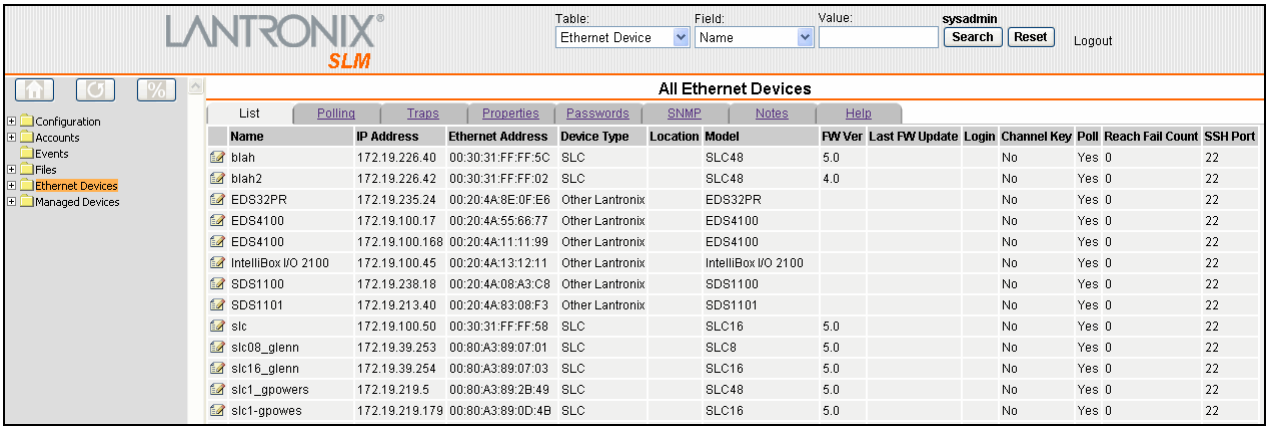
You can view a list of all devices in the SLM database. The list may include other Lantronix-built devices and even non-Lantronix devices.

Note: The examples in this section show SLCs. You can perform similar actions on all other Ethernet devices.

To list all devices on the network:

1. To view all of the detected devices, click **Ethernet Devices** on the menu. The All Ethernet Devices page displays all devices in the database.

Figure 8-2. All Ethernet Devices Page – List Tab



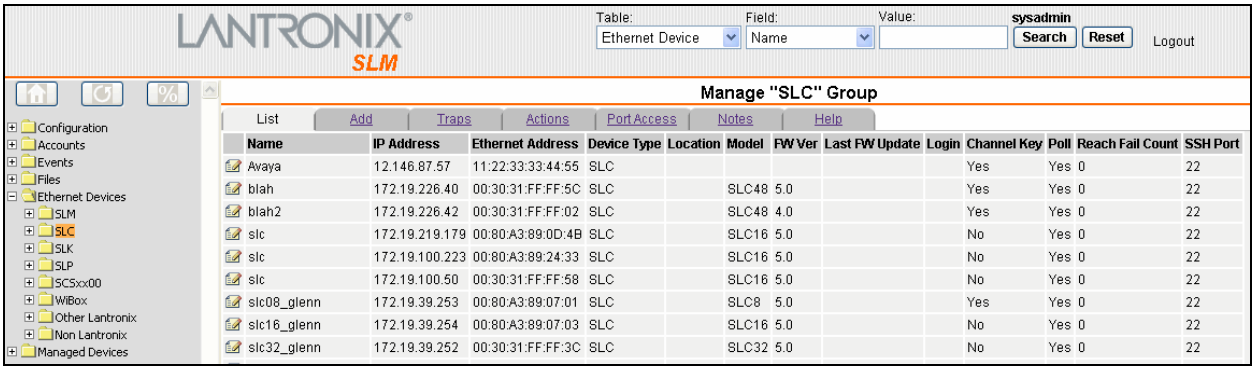
Name	IP Address	Ethernet Address	Device Type	Location	Model	FW Ver	Last FW Update	Login	Channel Key	Poll	Reach Fail Count	SSH Port
blah	172.19.226.40	00:30:31:FF:FF:5C	SLC		SLC48	5.0			No	Yes	0	22
blah2	172.19.226.42	00:30:31:FF:FF:02	SLC		SLC48	4.0			No	Yes	0	22
EDS32PR	172.19.235.24	00:20:4A:8E:0F:E6	Other Lantronix		EDS32PR				No	Yes	0	22
EDS4100	172.19.100.17	00:20:4A:55:66:77	Other Lantronix		EDS4100				No	Yes	0	22
EDS4100	172.19.100.168	00:20:4A:11:11:99	Other Lantronix		EDS4100				No	Yes	0	22
IntelliBox I/O 2100	172.19.100.45	00:20:4A:13:12:11	Other Lantronix		IntelliBox I/O 2100				No	Yes	0	22
SDS1100	172.19.238.18	00:20:4A:08:A3:C8	Other Lantronix		SDS1100				No	Yes	0	22
SDS1101	172.19.213.40	00:20:4A:83:08:F3	Other Lantronix		SDS1101				No	Yes	0	22
slc	172.19.100.50	00:30:31:FF:FF:58	SLC		SLC16	5.0			No	Yes	0	22
slc08_glenn	172.19.39.253	00:80:A3:89:07:01	SLC		SLC8	5.0			No	Yes	0	22
slc16_glenn	172.19.39.254	00:80:A3:89:07:03	SLC		SLC16	5.0			No	Yes	0	22
slc1_gpowers	172.19.219.5	00:80:A3:89:2B:49	SLC		SLC48	5.0			No	Yes	0	22
slc1-gpowes	172.19.219.179	00:80:A3:89:0D:4B	SLC		SLC16	5.0			No	Yes	0	22

*Note: You can sort tables in SLM by clicking the text in the column header by which you want to sort. For example, to sort by name, click **Name.** Click the same header again to change between ascending and descending order. If there is more data in a table than fits on the screen, scroll forward and backward through the data.*

To list all Ethernet devices of a specific type:

- To list all SLCs managed by the SLM, click **Ethernet Devices→SLC** on the menu tree. The following page opens:

Figure 8-3. Manage Group Page – List Tab


LANTRONIX
SLM
Table: Ethernet Device
Field: Name
Value:
sysadmin
Search
Reset
Logout
Manage "SLC" Group
List
Add
Traps
Actions
Port Access
Notes
Help
Configuration
Accounts
Events
Files
Ethernet Devices
SLM
SLC
SLK
SLP
SCSxx00
WiBox
Other Lantronix
Non Lantronix
Managed Devices
Name | IP Address | Ethernet Address | Device Type | Location | Model | FW Ver | Last FW Update | Login | Channel Key | Poll | Reach Fail Count | SSH Port
Avaya | 12.146.87.57 | 11:22:33:33:44:55 | SLC | Yes | Yes | 0 | 22
blah | 172.19.226.40 | 00:30:31:FF:FF:5C | SLC | SLC48 | 5.0 | Yes | Yes | 0 | 22
blah2 | 172.19.226.42 | 00:30:31:FF:FF:02 | SLC | SLC48 | 4.0 | Yes | Yes | 0 | 22
slc | 172.19.219.179 | 00:80:A3:89:0D:4B | SLC | SLC16 | 5.0 | No | Yes | 0 | 22
slc | 172.19.100.223 | 00:80:A3:89:24:33 | SLC | SLC16 | 5.0 | No | Yes | 0 | 22
slc | 172.19.100.50 | 00:30:31:FF:FF:58 | SLC | SLC16 | 5.0 | No | Yes | 0 | 22
slc08_glenn | 172.19.39.253 | 00:80:A3:89:07:01 | SLC | SLC8 | 5.0 | Yes | Yes | 0 | 22
slc16_glenn | 172.19.39.254 | 00:80:A3:89:07:03 | SLC | SLC16 | 5.0 | No | Yes | 0 | 22
slc32_glenn | 172.19.39.252 | 00:30:31:FF:FF:3C | SLC | SLC32 | 5.0 | No | Yes | 0 | 22

- To list devices in any other device group (e.g., SLK, SLP, or Other Lantronix), click **Ethernet Devices** and the name of the device group on the menu tree.

Adding a Device Manually

If you know there is a new device on the network, or for some reason, the SLM does not auto-detect a device, the administrator can manually add it.

To add a device:

Note: *Ethernet device pages may differ slightly, depending on the type of device. The procedure below the examples notes these differences.*

1. On the menu tree, click **Ethernet Devices** and then the type of device you are adding (e.g., SLC, SLK, Spider, or Other Lantronix).
2. Click the **Add** tab. Depending on the device type, one of the following pages or a similar page displays.

Note: *The connection buttons on the right are inactive until the Ethernet device has been added to the system.* See *Connecting to Ethernet and Managed Devices on page 187* *for instructions on using the buttons.*

Figure 8-4. Add SLM Device Page – Configure Tab

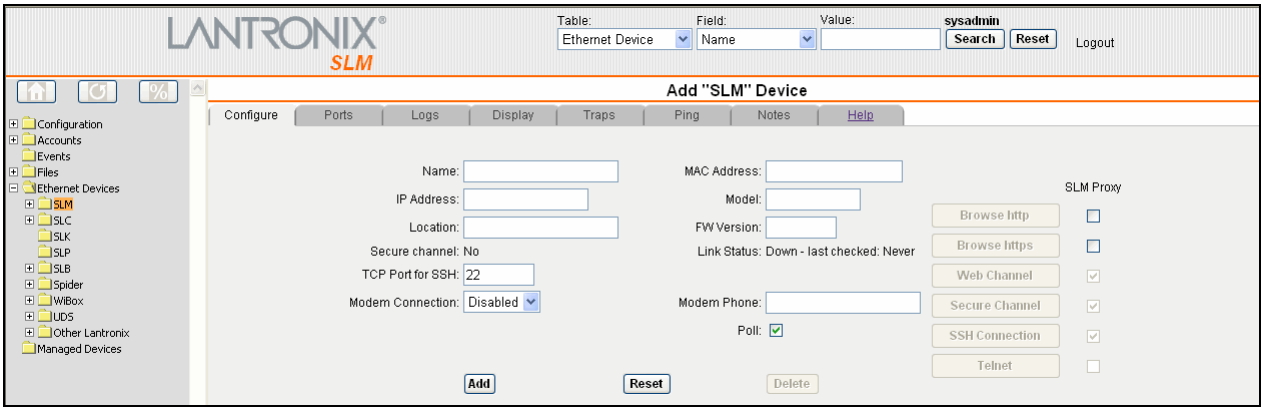


Figure 8-5. Add SLC Device Page – Configure Tab

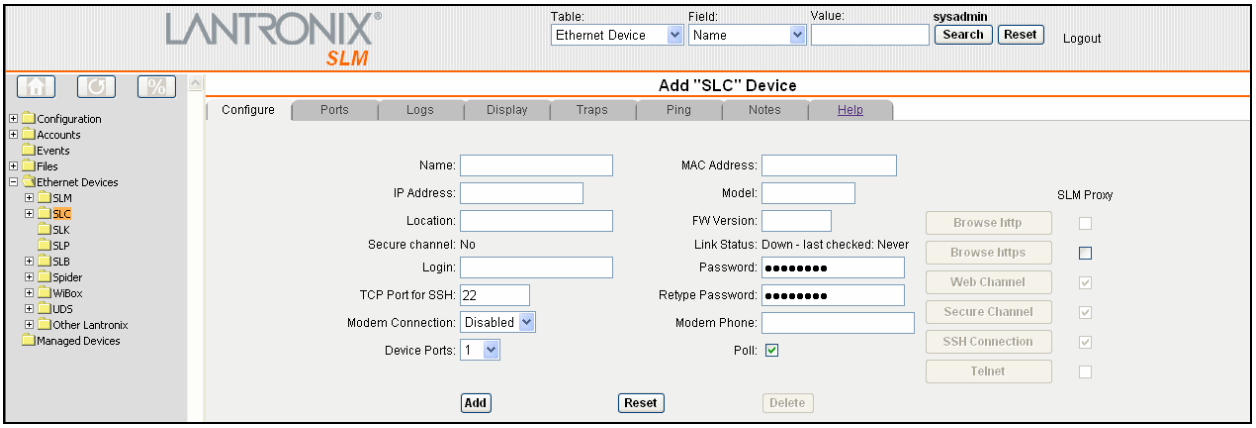


Figure 8-6. Add Spider Device Page – Configure Tab

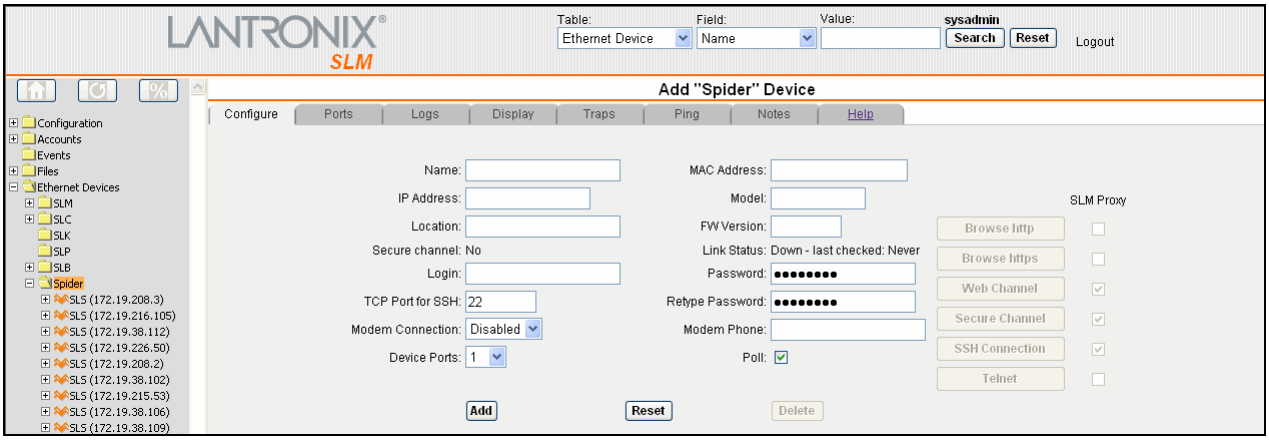
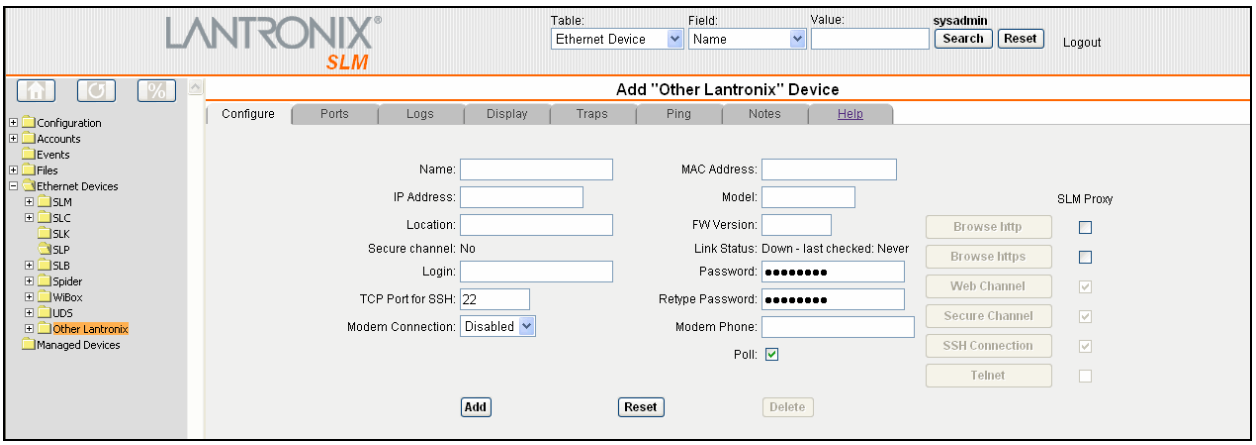


Figure 8-7. Add Other Lantronix Device Page – Configure Tab



3. Enter the following as required by the device type:

Name (required)	Name that identifies the device.

MAC Address (required)	Network (Ethernet) number of the device (on the device label). ***Note:*** *Enter all Ethernet addresses in hexadecimal, colon-separated format (e.g., 12:34:56:AB:CD:EF).*
IP Address (required)	IP address that uniquely identifies the device on the network. There is no default. ***Note:*** *Enter all IP addresses in dot quad notation.*
Model	Model number of the device. Required for an SCS05/20.
Location	Place where the device is installed (e.g., city, building, or room).
FW Version	Release number of the firmware.
Secure Channel (view only)	Indicates whether the SLM has a Lantronix secure channel connection from the web interface to the command line interface of an SLC and its ports. The default is **No**.
Link Status (view only)	Indicates whether or when the SLM polled the connection from the SLM to the device.
Login (not on SLM)	User name for logging into any Ethernet device that can be logged into using http or https.
Password and **Retype Password** (not on SLM)	Password for logging into any Ethernet device that can be logged into using http or https.
TCP Port for SSH	Number of the port for establishing an SSH connection to the device or its ports. The default setting is **22**.
Modem Connection	From the drop-down list, select the status of the connection. The default setting is **Disabled**.
Modem Phone	The phone number that the device calls.
Poll	If selected, the SLM will include this device when performing periodic polling of Ethernet devices. Selected by default.
SLM Proxy	If selected, connections of the specified type created between the client and the Ethernet device will be proxied through the SLM rather than established directly.

4. Click the **Add** button.
5. Click **Ethernet Devices** and then the device group (e.g., SLC) to which you added the device. The added device displays at the end of the list and on the menu tree.

Updating or Deleting Ethernet Device Settings

The Administrator and Ethernet Device Account groups can edit settings for SecureLinx management devices (SLCs, SLBs, SLKs, SLPs, SLBs, Spiders, and other SLMs) and other Ethernet devices. They can also delete a device from the SLM database so that the SLM will no longer manage it.

To update an Ethernet device:

1. On the All Ethernet Devices or the Manage Group page, click the **Edit** icon to the left of the desired device,

   OR

On the menu tree, click the name of the desired device. The **Configure** tab for the device opens.

*Note: Examples of the SLC, SLP, and SLK **Configure** tabs are shown below.*

Figure 8-8. SLC Device Page – Configure Tab

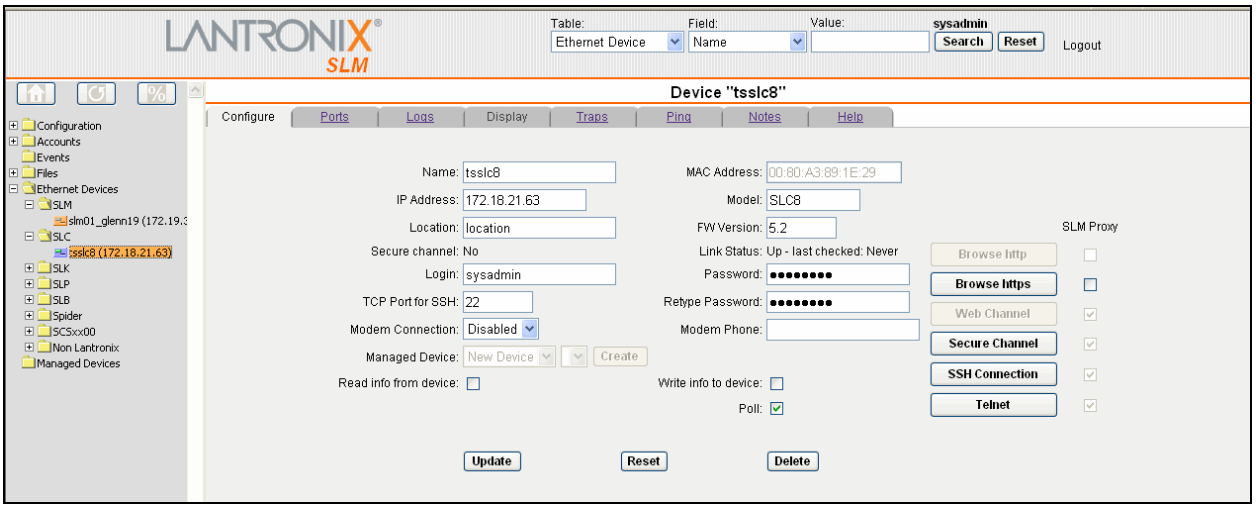


Figure 8-9. SLP Device Page – Configure Tab

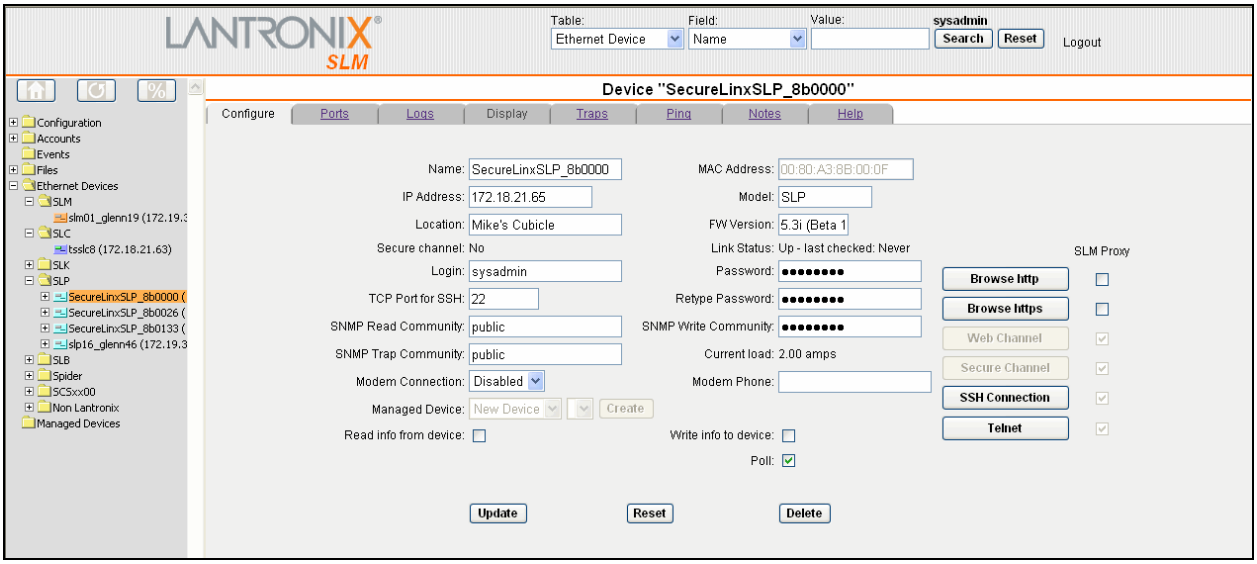
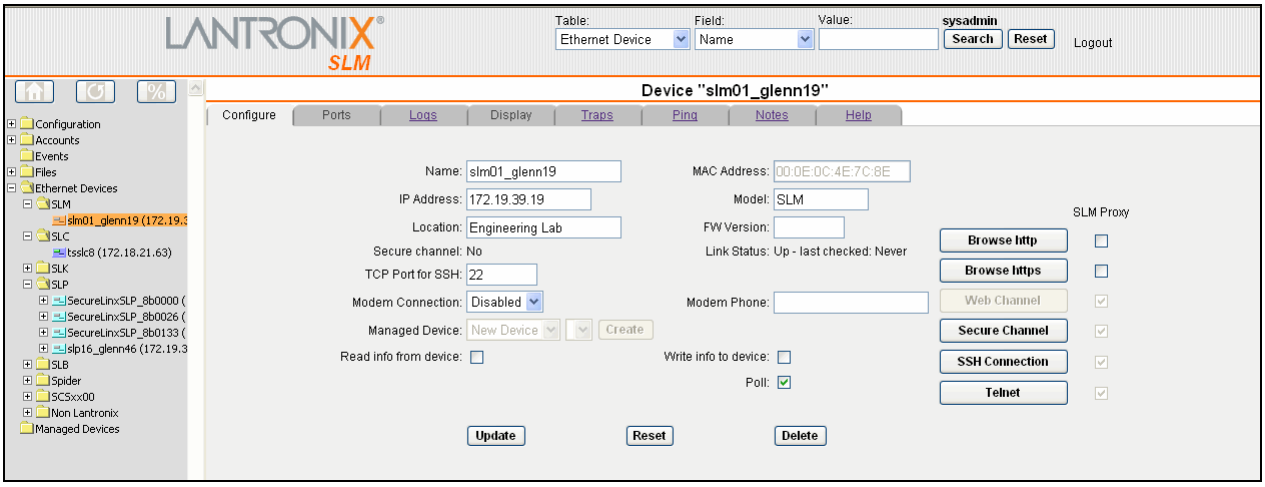


Figure 8-10. SLM Device Page – Configure Tab



Note: See Connecting to Ethernet and Managed Devices on page 187 for instructions on how to use the active connect buttons.

2. Add or update information as desired. In addition to the fields described on page 125, enter the following for SLCs, SLBs, SCSs, SLMs, and SLPs:

Managed Device	If desired, create a managed device from the Ethernet device. For more information, see *Creating Individual Managed Devices* on page 164. *Note: This field is unavailable if no Managed Device Groups exist in the system.*
Read info from device	If selected, the SLM will attempt to update its internal database by interrogating the physical device. The SLM must have a Secure Channel established to the Ethernet device (or provide the sysadmin login and password of the Ethernet devices) for this function to work. Currently, the SLM can read the following information: **SLC:** SLC host name, firmware version, device port names, device port parameters (e.g. baud, flow control), and the SLM logging parameters for each port **SCSxx05/20:** SCS host name and the port names **SLM:** SLM host name and firmware version **SLP:** SLP outlet names and outlet IDs **SLB:** SLB host name, firmware version, device port names, device port parameters (e.g. baud, flow control), and the SLM logging parameters for each port

Write info to device	If selected, the SLM will attempt to update the physical device using the values currently in its internal database. The SLM must have a Secure Channel established to the Ethernet device (or provide the sysadmin login and password of the device) for this function to work. Currently, the SLM can write the following information: **SLC:** SLC host name, device port names, device port parameters (e.g. baud, flow control), and the SLM logging parameters for each port **SCSxx05/20:** SCS port names **SLM:** SLM host name **SLP:** SLP outlet name **SLB:** SLB host name, device port names, device port parameters (e.g. baud, flow control), and the SLM logging parameters for each port

3. Click the **Update** button. When the update is complete, a confirmation message displays.

To delete the device:

1. Click the **Delete** button.
2. In response to the request for confirmation, click **OK**. A blank device page opens.
3. Click **Ethernet Devices** on the menu tree. The deleted device is no longer on the menu tree or listed on the Device Group page.

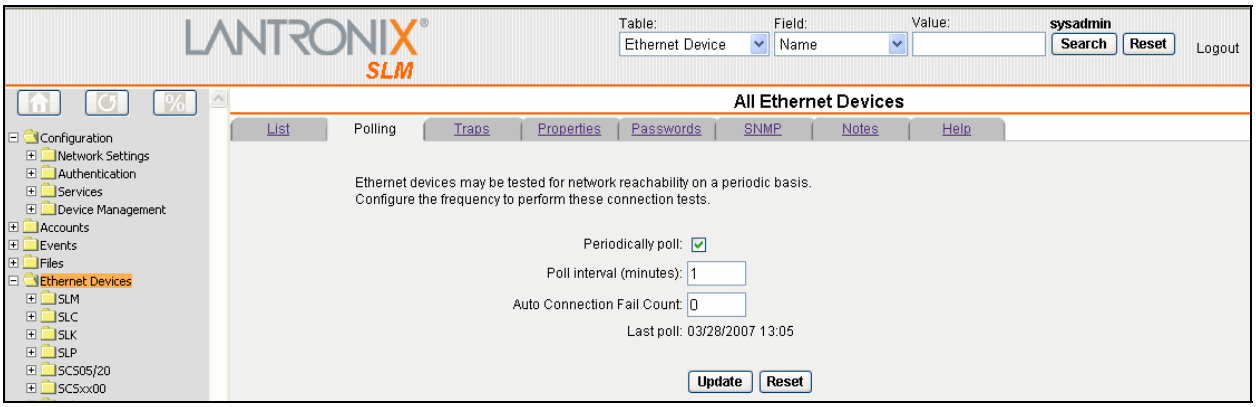
Polling

Only administrators with **Allow Device Management** set on their account page can access the global polling page. Any administrator or Ethernet device user with rights to an Ethernet device can change the "poll flag" for the device. This poll flag enables and disables polling on a device-by-device basis. The poll flag of a device is enabled by default, but if not selected, even if polling is turned on, that device will not be polled.

To poll Ethernet devices on the network:

1. On the menu, click **Ethernet Devices**. The All Ethernet Devices page opens.
2. Click the **Polling** tab. The following page opens.

Figure 8-11. All Ethernet Devices -- Polling Tab



3. Enter the following information:

Periodically poll	Select to have the SLM poll Ethernet devices on the network at regular intervals. Disabled by default. If you select this option, then any Ethernet device that has its "poll" flag set but fails to respond to Auto Connection Fail Count consecutive polling attempts displays with a vertical red stripe in its icon on the menu tree. ***Note:*** *You can disable polling on a per device basis by clearing the poll flag on an individual device's page.*
Poll interval (minutes)	Number of minutes the SLM should wait between polls.
Auto Connection Fail Count	The following conditions are required for the SLM to automatically connect to the SLC through a modem: ◆ Ethernet device polling is enabled. ◆ The SLC device has polling enabled for itself. ◆ The SLC has a modem connection and phone number configured. ◆ The SLC has reached the maximum polling failure count (see below). ◆ There is an available modem on the SLM. Enter the number of consecutive times the system must fail to reach the SLC before the SLM will connect through a modem. Enter **0** (zero) to disable this feature. Once the connection is established, it will remain connected until after either a successful Ethernet poll or a manual disconnect of the modem by an SLM user.
Last poll (view only)	Time the last poll was performed.

4. To save, click the **Update** button. A confirmation message displays.

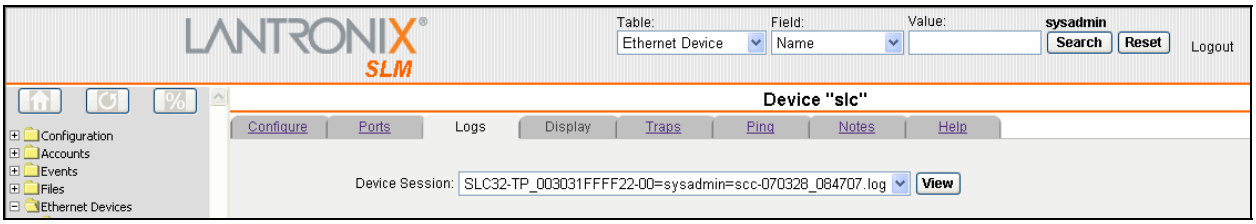
Viewing Session Log Files

On the Device page, you can view all session log files for the device.

To view session log files:

1. On the Device page, click the **Logs** tab. The following page opens:

Figure 8-12. Device Page – Logs Tab



Device session log file names have the following format:

<hostname>_<host_mac_address>-<device_port_number>=<username>=<connection_type>-<date_and_time>.log, where:

<hostname>	Up to the first 8 characters of the hostname of the Ethernet device. If the hostname is shorter than 8 characters, the hostname section is padded with ~ characters to reach this length.
<host_mac_address>	MAC Address of the Ethernet device. This is used by the SLM to correlate log files to their corresponding Ethernet devices.
<device_port_number>	Device port number connected to for this session. This field is set to 0 "00" for direct connections to the Ethernet device.
<username>	The SLM user ID that initiated this session.
<connection_type>	Session connection type: **tnt** for telnet, **ssh** for ssh, or **scc** for secure channel.
<date_and_time>	Date and time string in the format YYMMDD_HHMMSS

2. From the **Device Session** drop-down list, select the log you want to view.
3. Click the **View** button. The contents of the log display on the **Display** tab.

Note: *For information about a global option for enabling both device session logging and SLC port session logging, see Services on page 196.*

Traps

Traps are notifications of events sent from one device to another. The traps listed below are those sent by other devices (SLMs, SLCs, SLPs, and SLKs) and received by the SLM. This feature is applicable when you select **Enable Traps Reception** on the SNMP Agent page. Examples of traps the SLM can receive include:

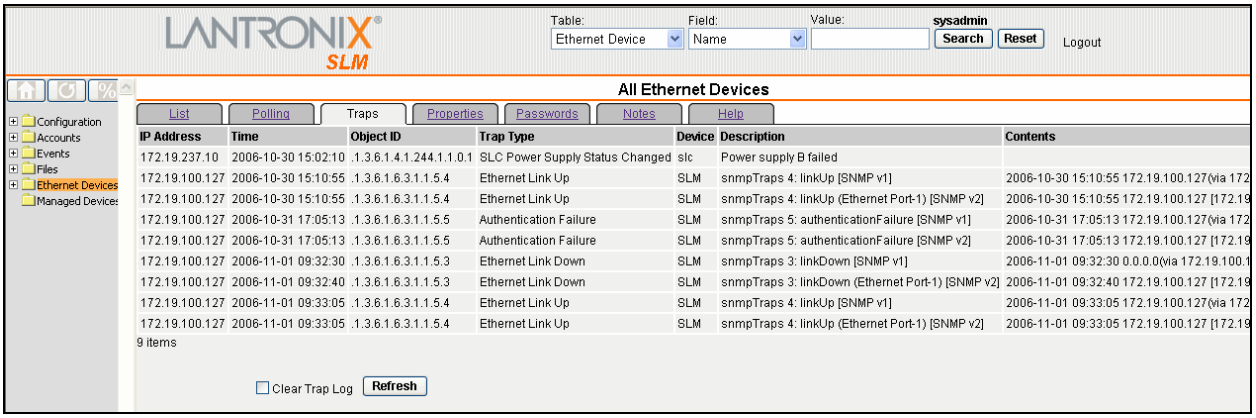
- SNMP Generic Traps:
  - Cold Start
  - Warm Start
  - Ethernet Link Down
  - Ethernet Link Up
  - Authentication Failure
  - EGP Neighbor Loss
- SLM Custom Traps (specified in SLM custom MIBs)
- SLC Custom Traps (specified in SLC custom MIBs)
- SLP Custom Traps (specified in SLP custom MIBs)
- SLK Custom Traps (specified in SLK custom MIBs)

Note: *You can view traps on three levels: All Ethernet devices, Ethernet device group, and individual Ethernet device.*

To view traps for devices listed on the All Ethernet Devices page:

1. On the menu, click **All Ethernet Devices**, the Ethernet device group, or the individual device, and then click the **Traps** tab. The following page opens.

Figure 8-13. All Ethernet Devices Page -- Traps Tab


LANTRONIX SLM
Table: Ethernet Device
Field: Name
Value:
sysadmin
Search
Reset
Logout
Configuration
Accounts
Events
Files
Ethernet Devices
Managed Devices
All Ethernet Devices
List
Polling
Traps
Properties
Passwords
Notes
Help
IP Address | Time | Object ID | Trap Type | Device | Description | Contents
172.19.237.10 | 2006-10-30 15:02:10 | .1.3.6.1.4.1.244.1.1.0.1 | SLC Power Supply Status Changed | slc | Power supply B failed
172.19.100.127 | 2006-10-30 15:10:55 | .1.3.6.1.6.3.1.1.5.4 | Ethernet Link Up | SLM | snmpTraps 4: linkUp [SNMP v1] | 2006-10-30 15:10:55 172.19.100.127(via 172
172.19.100.127 | 2006-10-30 15:10:55 | .1.3.6.1.6.3.1.1.5.4 | Ethernet Link Up | SLM | snmpTraps 4: linkUp (Ethernet Port-1) [SNMP v2] | 2006-10-30 15:10:55 172.19.100.127 [172.19
172.19.100.127 | 2006-10-31 17:05:13 | .1.3.6.1.6.3.1.1.5.5 | Authentication Failure | SLM | snmpTraps 5: authenticationFailure [SNMP v1] | 2006-10-31 17:05:13 172.19.100.127(via 172
172.19.100.127 | 2006-10-31 17:05:13 | .1.3.6.1.6.3.1.1.5.5 | Authentication Failure | SLM | snmpTraps 5: authenticationFailure [SNMP v2] | 2006-10-31 17:05:13 172.19.100.127 [172.19
172.19.100.127 | 2006-11-01 09:32:30 | .1.3.6.1.6.3.1.1.5.3 | Ethernet Link Down | SLM | snmpTraps 3: linkDown [SNMP v1] | 2006-11-01 09:32:30 0.0.0.0(via 172.19.100.1
172.19.100.127 | 2006-11-01 09:32:40 | .1.3.6.1.6.3.1.1.5.3 | Ethernet Link Down | SLM | snmpTraps 3: linkDown (Ethernet Port-1) [SNMP v2] | 2006-11-01 09:32:40 172.19.100.127 [172.19
172.19.100.127 | 2006-11-01 09:33:05 | .1.3.6.1.6.3.1.1.5.4 | Ethernet Link Up | SLM | snmpTraps 4: linkUp [SNMP v1] | 2006-11-01 09:33:05 172.19.100.127(via 172
172.19.100.127 | 2006-11-01 09:33:05 | .1.3.6.1.6.3.1.1.5.4 | Ethernet Link Up | SLM | snmpTraps 4: linkUp (Ethernet Port-1) [SNMP v2] | 2006-11-01 09:33:05 172.19.100.127 [172.19
9 items
Clear Trap Log
Refresh

2. Review the following information:

IP Address	IP address of the Ethernet device generating the trap.
Time	Time the Ethernet device generated the trap.
Object ID	Uniquely identifies the trap among all possible traps from all SNMP-capable devices; it is derived from the trap.
Trap Type	Category of trap, for example, device cold/warm start, device Ethernet link up/down, device authentication failure; it is derived from the trap.
Device	Name of the device sending the trap; it is derived by associating the sender's IP address to a device name in the SLM database.
Description	Message text in the trap.
Contents	The entire contents of the SNMP trap.

3. To clear the table, click the **Clear Trap Table** button.

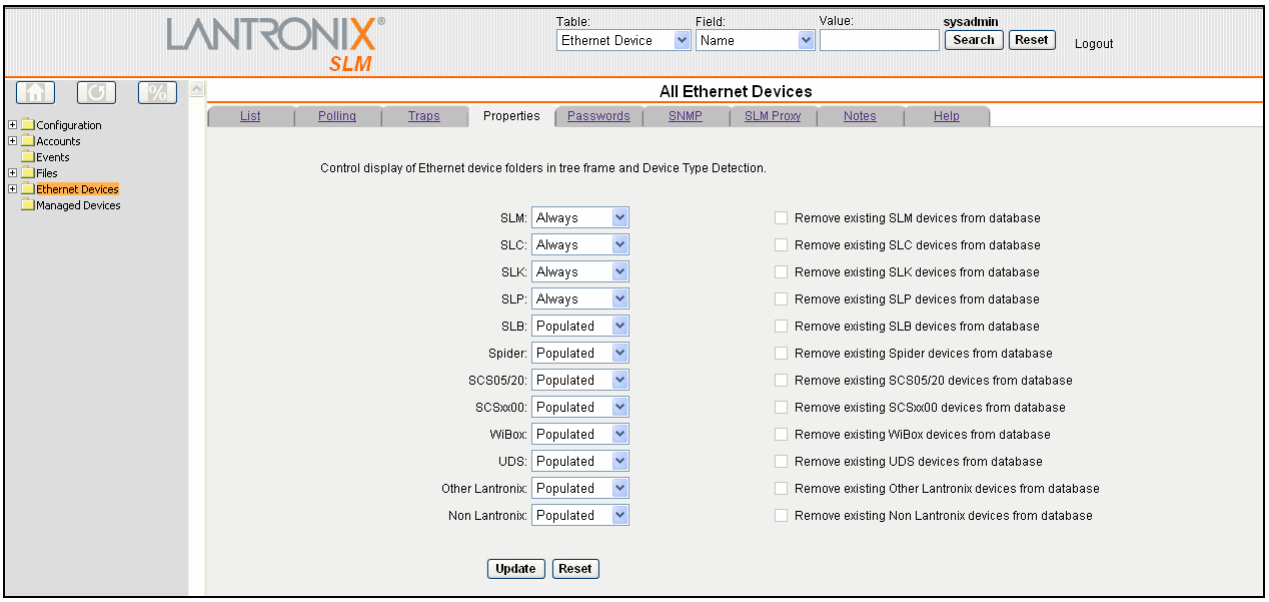
Properties (Ethernet Device Menu Tree)

The system administrator can control the display of Ethernet device folders in the tree menu.

To configure the Ethernet device menu tree:

1. Click the **Properties** tab. The following page opens:

Figure 8-14. All Ethernet Devices Page -- Properties Tab



2. Enter the following:

Ethernet Device Groups	For each device group, select one of the following options from the drop-down list: **Always:** Device folder displays whether populated or not. This is the default setting for the SLM, SLC, SLK, and SLP folders. **Never:** Device folder does not display, even if populated. **Populated:** Device folder displays only when populated. This is the default setting for the SCS05/20, SCSxx00, BoBox, Spider, WiBox, Other Lantronix, and Non Lantronix folders. **Don't Detect:** Prevents devices of this type from being auto detected.

3. To remove all devices of a type currently in the SLM database, select its checkbox.

   Note: *Check boxes are active only if you change the display mode to* ***Don't Detect****.*

4. To save, click the **Submit** button.

Port Access

The Port Access tab is available for SLCs, SLBs, SLPs, and Spiders and provides the following:

SLCs: Connection to serial ports.

SLBs: Connection to serial ports and access to the port page for power ports.

SLPs: Access to the port page for power ports.

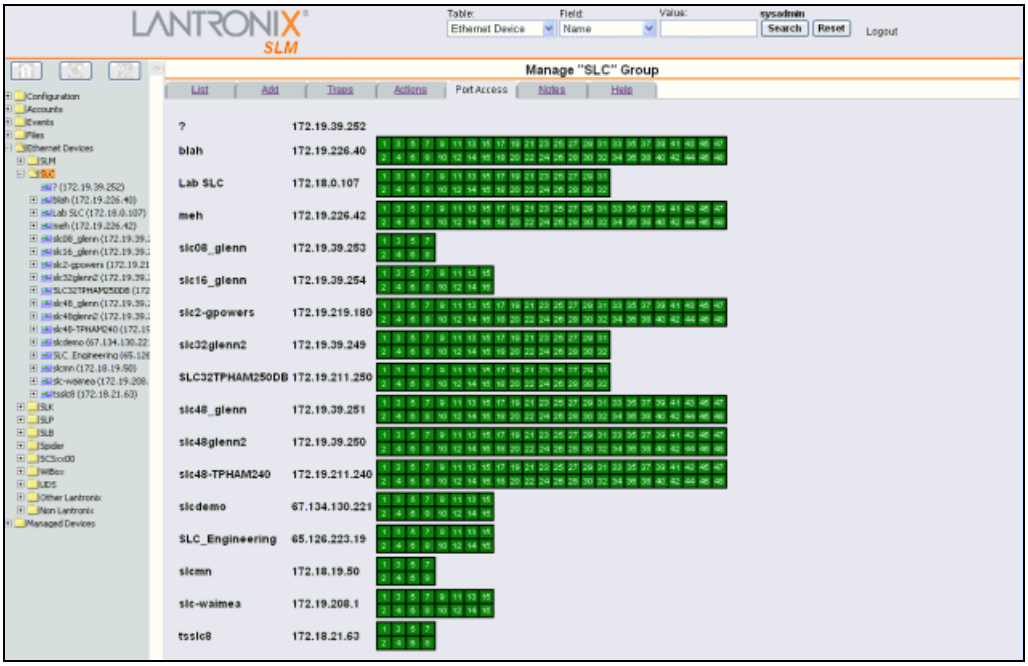
Spiders: KVM access to devices connected to a Spider.

To connect to an SLC port:

1. On the menu, click **Ethernet Devices > SLC.** The Manage SLC Group page opens.
2. Click the **Port Access** tab. A list of all SLCs displays, along with all of their ports. Numbered squares represent the ports.

   Note: *Hovering over a port reveals the port name*.

Figure 8-15. Manage SLC Group -- SLC Tab



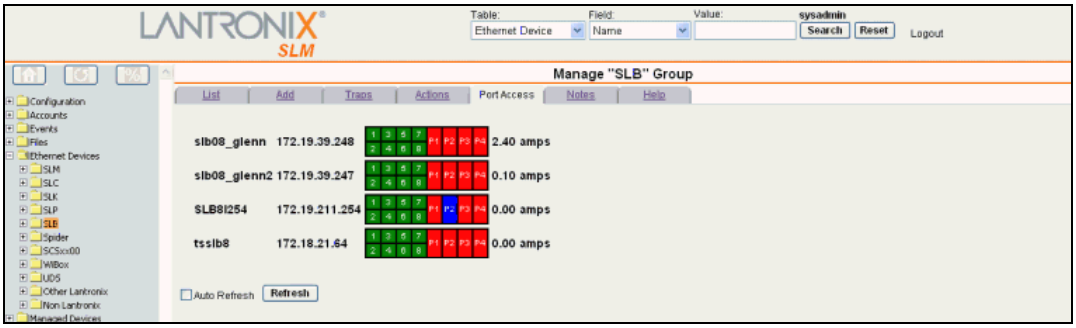
3. Click the SLC port to open a Secure Channel connection.

To connect to an SLB port or access its port page:

1. On the menu, click **Ethernet Devices > SLB**. The Manage SLB Group page displays:
2. Click the **Port Access** tab. A list of all SLBs and their IP addresses displays, along with all of their ports and the power load of each port.

   Note: *Hovering over a port reveals the port name*.

Figure 8-16. Mange SLB Group – Port Access Tab



Color-coded numbered squares represent the ports:

- Green = serial ports
- Red = power port on
- Blue = power port off

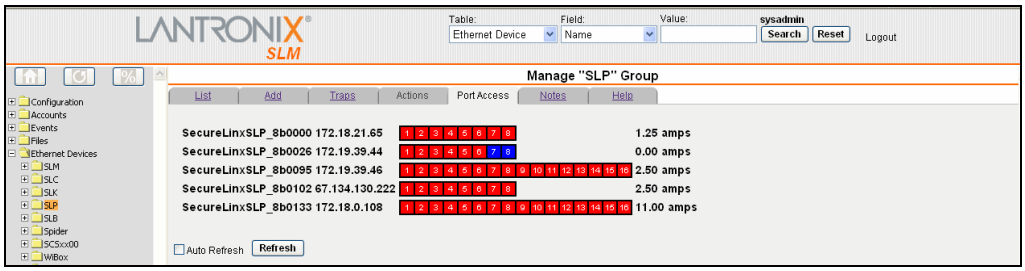
3. You have the following options:
   - To open a Secure Connection with a serial port, click the corresponding green square.
   - To open an SLB port page, click the corresponding red or blue square.

To access an SLP port page:

1. On the menu, click **Ethernet Devices > SLP**. The Manage SLP Group page displays:
2. Click the **Port Access** tab. A list of all SLPs displays, along with all of their ports and the power load of each port.

   Note: *Hovering over a port reveals the port name*.

Figure 8-17. Manage SLP Group – Port Access Tab



Color-coded numbered squares represent the ports:

- Blue = power port off
- Red = power port on
- Grey = state unknown

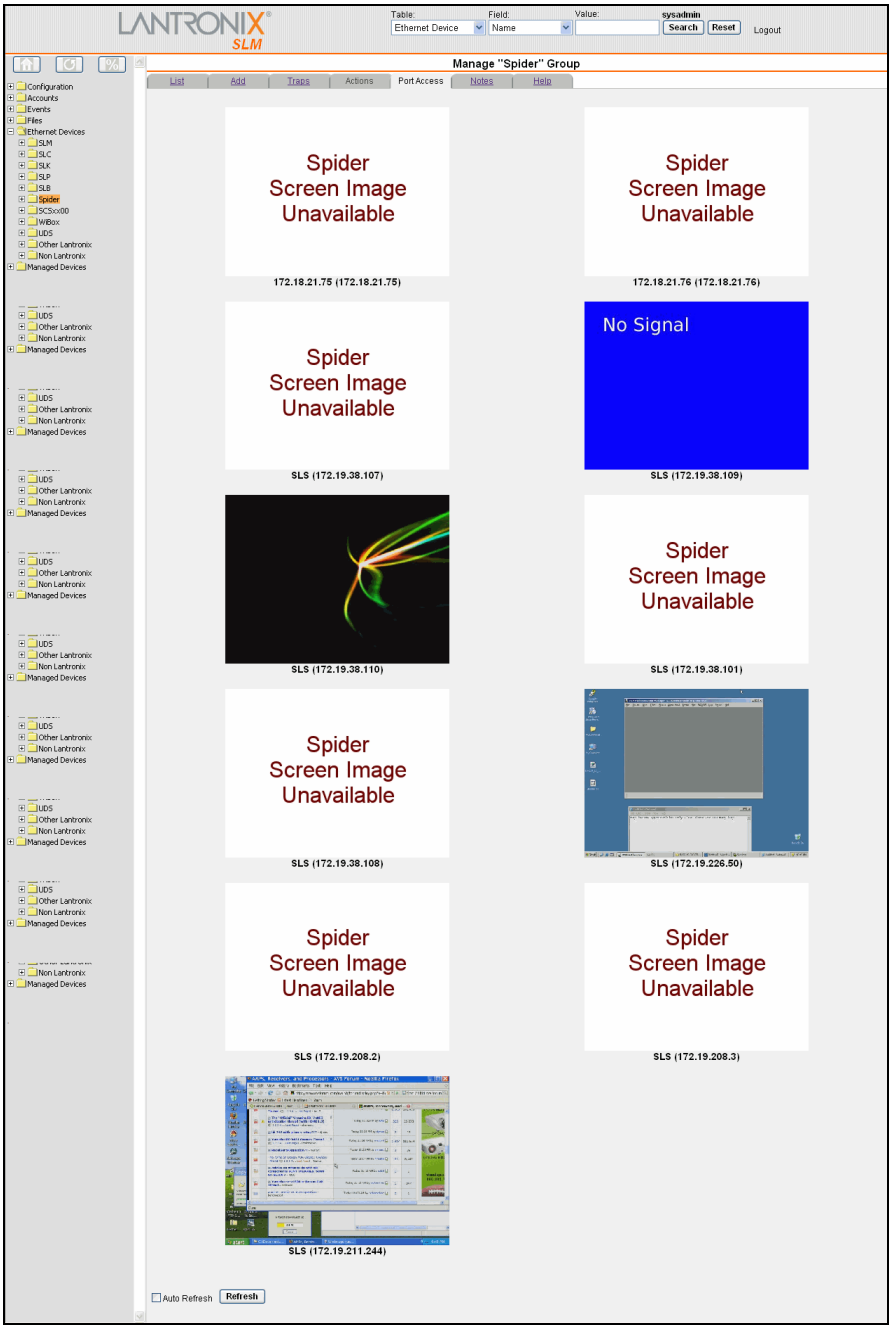
3. Click the port whose port page you want to open.

To gain KVM access to a device connected to a Spider:

1. On the menu, click **Ethernet Devices > Spider**. The Manage Spider Group page displays.

2. Click the **Port Access** tab. All Spiders in the system display as boxes with IP addresses. Some boxes may display the current view of the device the Spider is controlling.

Figure 8-18. Manage Spider Group – Port Access Tab



3. Click the screen image to open a Spider KVM session to that device.

To refresh the Port Access tab:

1. You have two options:
   - To refresh the port information automatically every two minutes, select the **Auto Refresh** check box and click the **Refresh** button.

- To refresh the port information once, clear the **Auto Refresh** check box and click the **Refresh** button.

Updating Passwords in Bulk

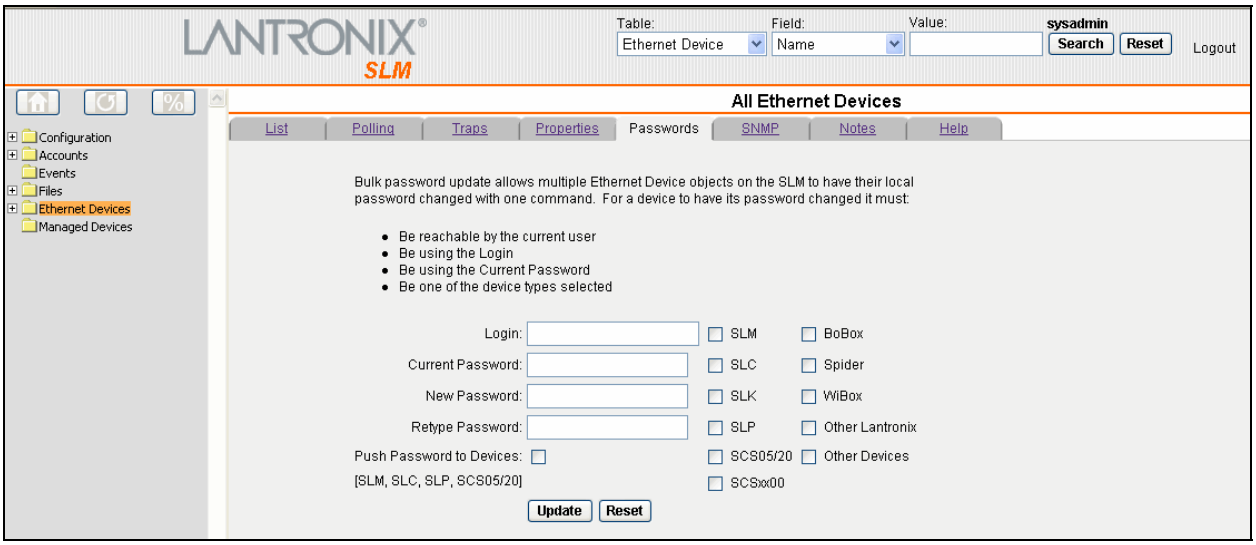
The administrator and Ethernet device users can perform bulk password updates on multiple devices in the local database. These changes can also be pushed to remote SLM, SLC, SLP, and SCS05/20 devices.

- The user has access to the device.
- The current user ID on the device matches the **Login** field.
- The current password on the device matches the **Current Password** field.
- The device type matches one of the types selected on the page described below.

To perform a bulk password update:

1. On the menu, click **Ethernet Devices** and then the **Passwords tab**. The following page opens:

Figure 8-19. All Ethernet Devices Page – Passwords Tab



2. Enter the following:

Login	Enter the login currently used by the devices whose password you want to change.
Current Password	Enter the password currently used by the devices whose password you want to change.
New Password and **Retype Password**	Enter a new password for accessing the devices.
SLM, SLC, SLK, SLP, SCS05/20, SCSxx00, SLB, Spider, WiBox, UDS, Other Lantronix, Other devices	Select the check box for each type of device whose password you want to change.

Push Passwords to Devices	Select the checkbox when you want to push the password change to remote SLM, SLC, SLP, and SCS05/20 devices.

3. Click the **Update** button. A confirmation message displays.

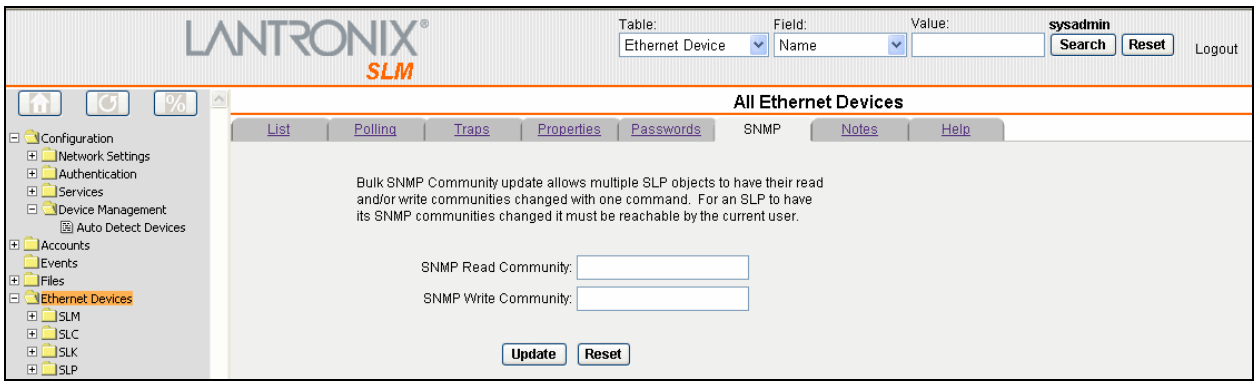
Changing SNMP Settings for SLPs in Bulk

For security reasons, some companies change SNMP communities frequently. The administrator can change the SNMP communities for multiple SLPs at the same time. To change the SNMP communities of an SLP, the current user must be able to access it.

To perform a bulk SNMP update:

1. On the menu, click **Ethernet Devices** and then the **SNMP** tab. The following page opens:

Figure 8-20.All Ethernet Devices Page – SNMP Tab



2. Enter the following:

SNMP Read Community	An SNMP community is the group to which devices and management stations running SNMP belong. The default setting is **public**. ***Note:*** *Because SSH-to-SLP authentication may take a long time, this setting allows the user to choose SNMP support, which is faster.*
SNMP Write Community	A string that acts like a password for an SNMP manager to modify data where permitted.

3. Click the **Update** button. A confirmation message displays.

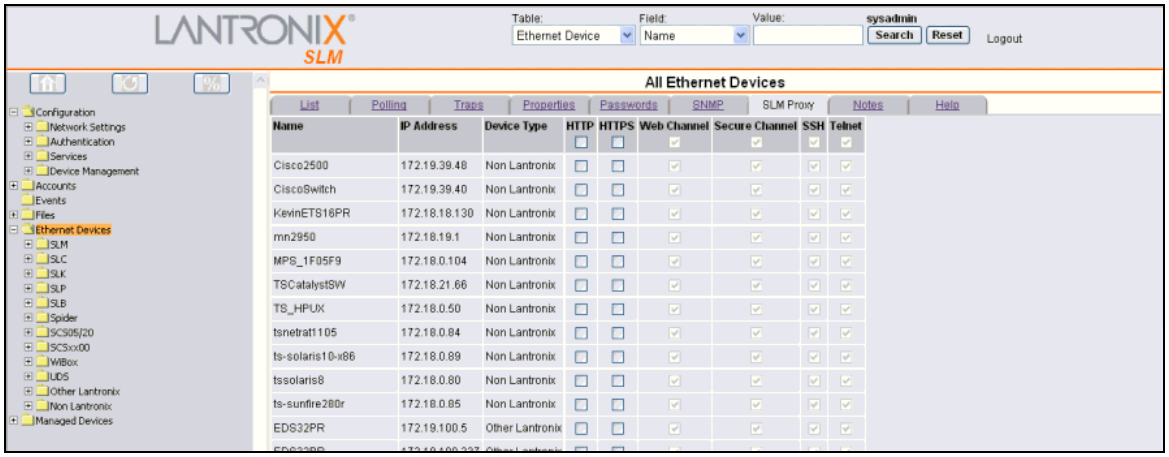
SLM Proxy

The SLM can act as a proxy server, allowing users outside the internal network to connect to devices securely through the SLM. You can set most devices to connect through the SLM. The SLM proxy feature is not limited to connections between the SLM's two Ethernet ports; the remote device can even be located on the same subnet as the client browser.

To use the SLM as a proxy server:

1. On the menu, click **Ethernet Devices**. The All Ethernet Devices page displays.
2. Click the **SLM Proxy** tab. The tab displays a list of all the Ethernet Devices with a column for each method of connection.

Figure 8-21. All Ethernet Devices – SLM Proxy Tab



Three types of check boxes display on the page:

- Active check boxes in the HTTP and HTTPS columns
- Selected check boxes that you cannot change because the devices are automatically set for proxy
- Blank check boxes or devices that cannot be set for proxy

3. To enable a device to use the SLM as a proxy in conjunction with HTTP or HTTPS, select the appropriate checkbox.

Note: *You may select* ***Proxy*** *in conjunction with these protocols and others on the configuration page for an individual device.*

Ethernet Device Commands

`set ethernetdevice config`

Syntax

```
set ethernetdevice config <Device Name or IP Address> <one or more parameters>
```

Parameters

```
[name <Device Name>]

[ipaddr <IP Address>]

[location <Location>]

[login <Loginname>]

[model <Model>]

[sshport <TCP Port for SSH>]

[version <Version>]
```

Description

Finds Ethernet devices by device name or IP address and modifies device parameters.

set ethernetdevice port

Syntax

```
set ethernetdevice port <Device Name or IP Address> portnumber
<Port Number> <one or more parameters>
```

Parameters

`[name <New Port Name>]`

`[state <on|off|cyclepower>]` (available for SLP only)
Powers Ethernet device port on or off.

Examples

To power up SLP outlet 2:

```
set eth port slp-sunset po 2 state on
```

You may specify a comma separated outlet list to control multiple outlet at once.

To power up SLP outlet port list 1-3,6,8-14:

```
set eth port slp-sunset po 1-3,6,8-14 state on
```

Description

Finds a port by device name or IP address with the port number and modifies port parameters.

set ethernetdevice sync

Syntax

```
set ethernetdevice sync <Device Name or IP Address> action
<read|write>
```

Description

Finds an Ethernet device using device name or IP address and synchronizes device information.

show device

Note: *Entries are not case sensitive.*

Syntax

```
show device <device name>
```

Description

Searches for and displays Ethernet or managed devices by device name.

show device all

Syntax

```
show device all
```

```
show device
```

Description

Displays all Ethernet and managed devices.

show ethernetdevice all

Syntax

```
show ethernetdevice all
```

Description

Displays all Ethernet device information.

show ethernetdevice config

Syntax

```
show ethernetdevice config <Device Name or IP Address>
```

Description

Finds an Ethernet device using device name or IP address and displays device information.

show ethernetdevice firmware

Syntax

```
show ethernetdevice firmware
```

Description

Displays firmware versions of all Ethernet devices managed by the SLM.

show ethernetdevice group

Syntax

```
show ethernetdevice group <Group Name> [firmware]
```

`group name`: SLM, SLC, SLK, SLP, SCS, LTRX, or other

Note: *Ethernet device group names are not case sensitive.*

Description

Displays Ethernet devices by device group.

show ethernetdevice index

Syntax

```
show ethernetdevice index <number>
```

Description

Displays Ethernet devices by index.

show ethernetdevice port

Syntax

```
show ethernetdevice port <Device Name or IP Address> all
```

```
show ethernetdevice port <Device Name or IP Address> portnumber
<Port Number>
```

Description

Finds an Ethernet device using device name or IP address and displays port information.

show ethernetdevice search device

Syntax

```
show ethernetdevice search device <one or more parameters>
```

Parameters

```
[name <Device Name>]
[ipaddr <IP Address>]
[location <location>] [firmware <version number>]
```

Note: *Search entries are not case sensitive.*

Example

```
show ethernetdevice search device name slc firmware 4
```

Description

Displays all devices that match the criteria entered. For example, if you specify `name slc`, the SLM searches for all devices whose name starts with `slc`.

Trap Commands

show traplog index

Syntax

```
show traplog [index <number>]
```

Description

Displays all current trap log information. The index number displays detailed information about a selected traplog.

show traplog device

Note: *Type `show traplog` to display the index.*

Syntax

```
show traplog device <Device Name or IP address> [index <number>]
```

Description

Displays the current trap log information for an Ethernet device using device name, IP address, or index number. `show traplog group`

show traplog group

Note: *Type `show traplog group` to display the index.*

Syntax

```
show traplog group <Device Group Name> [index <number>]
```

Group name: SLM, SLC, SLK, SLP, SCS, LTRX, or other

Description

Displays the current trap log information for an Ethernet device group by index number.

show traplog index

Syntax

`show traplog index <number> <parameters>`
`index` is the number of lines of the log specified by `lastminutes` and `date`. If you specify `0` at number of lines, all lines display.

Parameters

`[top <number of lines>]`

`[tail <number of lines>]`

`[lastminutes <minutes>]`

`[date <MMDD>]`

`[date <MMDD-MMDD>]`

`[loglastminutes <minutes>]`

`[logdate <MMDD>]`

`[logdate <MMDD-MMDD>]`

If you specify both the date and time, the SLM ignores the date.

Description

Displays the specified part of the traplog by index.

Examples

`show traplog`
Lists traplog files.

`show traplog lastminutes 5`
Lists traplog files modified in the last 5 minutes.

`show traplog date 0205`
Lists traplog files last modified on 0205.

`show traplog date 0205-0209`
Lists traplog files last modified between 0205 and 0209.

`show traplog index 3`
Displays index 3 from the top.

`show traplog index 3 top 10`
Displays the first 10 lines of index 3 from the top.

`show traplog index 3 tail 15`
Displays the last 15 lines of index 3 from the tail.

`show traplog index 3 lastminutes 5`
Displays the lines in index 3 from the last 5 minutes of.

`show traplog index 3 date 0205`
Displays the audit log in index 3 for the date 0205.

`show traplog index 3 date 0205-0209`
Displays the traplog by the index 3 between the dates 0205 to 0209.

`show traplog index 3 top 10 lastminutes 5`
Displays the first 10 lines of index 3 of the traplog from the last 5 minutes.

`show traplog index 3 tail 0 lastminutes 5`
Displays all lines of the traplog in index 3 from the tail.

```
show traplog index 3 lastminutes 5 logminutes 10
```
Displays the part of traplog in index 3 times tamped in the last 10 minutes.

```
show traplog index 3 date 0205
```
Displays the part of traplog in index 3 times stamped on 0205.

Ports

Administrators and Ethernet device users with rights to an Ethernet device can list, add, update, delete, and interact with its ports. Managed Device users can only interact with managed devices (which may manage one or more ports, and/or a local Ethernet device) that they have permissions on.

Note: *Port pages may differ slightly, depending on the type of Ethernet device. The procedures below note these differences.*

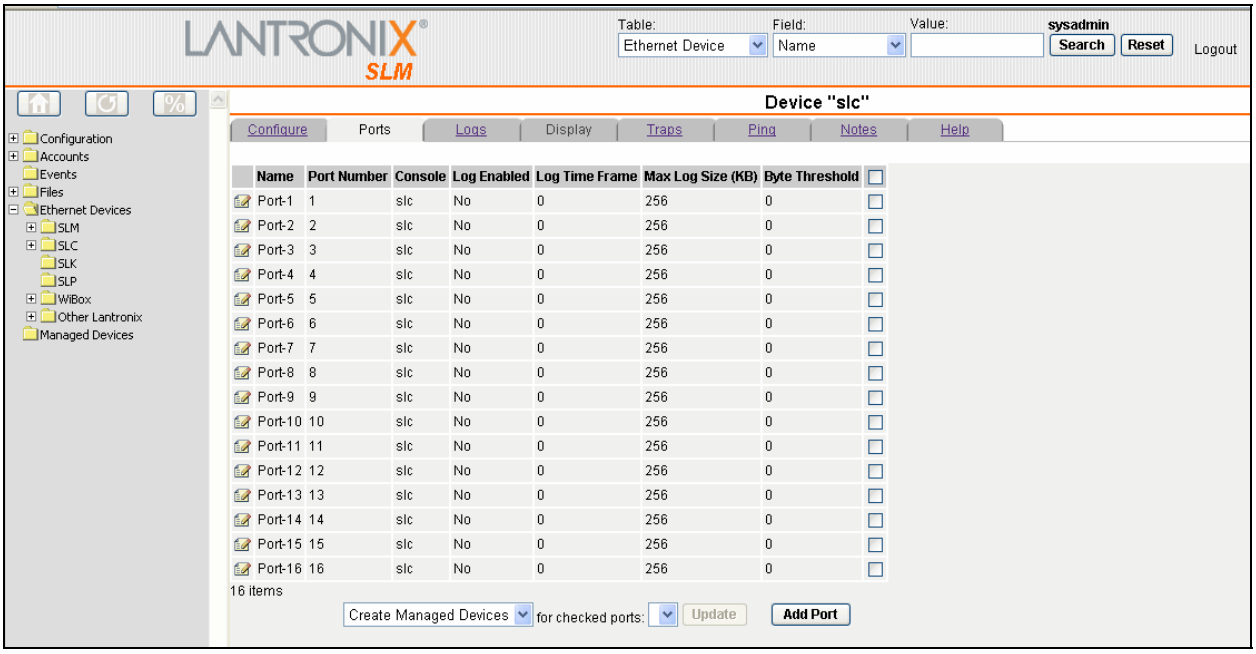
Viewing a List of Ports

You can view a list of all ports on any Ethernet device that has ports (e.g., SLC, SLK, SLP, and SCS).

To view port information:

1. On the Device page for the Ethernet device, click the **Ports** tab. The following page opens.

Figure 8-22. Device -- Ports Tab



2. View the following information about each port:

Name	Name of the Ethernet device port.
Port Number	Number of the Ethernet device port (e.g., a number between 1 and 48 for the SLC 48).
Console	Name of the Ethernet device.

Log Enabled	Indicates whether logging has been enabled for this port. ***Note:*** *To enable or disable port logging for one or more ports, select the check box for each affected port, and select* ***Enable Port Logging*** *or* ***Disable Port Logging*** *from the drop-down list at the bottom of the page.* *Only SLC devices that have established a secure channel connection can have ports with logging enabled.*
Log Time Frame	**For SLC v3.1 and later v3.x (but not v4.0):** The maximum time frame in *hours* before a new log file is created. The default setting is **1** hour. **For SLC v4.0 and later:** The maximum time frame *in seconds* before the SLC sends data to the SLM. The default is **30** seconds.
Max Log Size (KB)	Maximum size of each log file in kilobytes. Once it is reached, a new log file is created. The default setting is **256** KB.
Byte Threshold	**For SLC v4.0 and later:** The number of bytes the SLC device port receives before it forwards them to the SLM. For example, a threshold preset at 128 characters means that as soon as the SLC receives 128 bytes of data on this particular device port, it captures log data and sends it to the SLM. The minimum byte threshold is **1**, and the default is **1024**.
Port Status (SLP only)	Indicates whether the port's power is on or off.

Adding a Port

Administrators and Ethernet device users with rights to a device may add ports to that device. This is useful when a device does not automatically report port information.

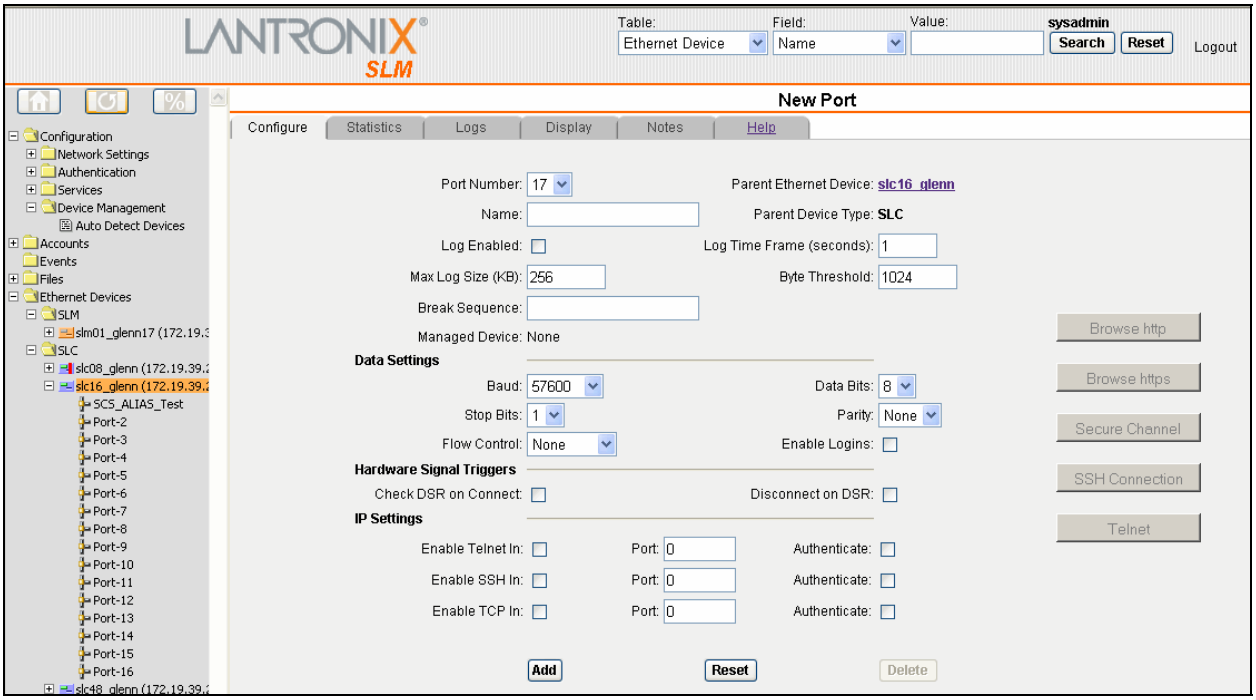
To add a port:

Notes:

- *The example below shows how to add an SLC port. Ports on other devices do not require extra port information such as baud and flow control).*
- *During auto detect, if an SLC device does not have SNMP enabled, it will not retrieve these extra SLC port parameters. Then this SLC device is marked with an internal flag to indicate that those port parameters are incorrect. When this flag is set, the user cannot perform a "Write info to device" as this would push incorrect port settings back to the SLC device. This flag is cleared if the user did a "Read info from device" or manually modified one of the SLC device port settings. After this flag is cleared, the user can perform "Write info to device."*

1. On the **Ports** tab of the Device page, click the **Add Port** button at the bottom. The following page opens:

Figure 8-23. New SLC Port Page – Configure Tab



***Note:** The connection buttons on the right are inactive until you save the port. (See Connecting to Ethernet and Managed Devices on page 187 for instructions on using the buttons.)*

2. Enter the following information:

Port Number	Number of the Ethernet device's port (e.g., a number between 1 and 48 for the SLC 48). The system offers all unassigned ports up to 16 above the current highest port number.
Parent Ethernet Device (view only)	Name of the Ethernet device.
Name	Name of the port (e.g., name of the device to which it is attached).
Parent Device Type (view only)	Ethernet device type (e.g., SLC, SLM, SLK).
Log Enabled	Indicates whether logging is enabled on the port. Disabled by default. ***Notes:*** ◆ To enable or disable port logging for one or more ports, select the check box for each affected port, and select **Enable Port Logging** or **Disable Port Logging** from the drop-down list at the bottom of the page. ◆ Only SLC devices that have established a secure channel connection can have ports with logging enabled.
Log Time Frame	**For SLC v3.1 and later v3.x (but not v4.0):** The maximum time frame in *hours* before a new log file is created. The default setting is **1** hour. **For SLC v4.0 and later:** The maximum time frame *in seconds* before the SLC sends data to the SLM. The default setting is **30** seconds.

Max Log Size (KB)	Maximum size of each log file in kilobytes. Once it is reached, a new log file is created. The default setting is **256** KB.
Byte Threshold	**For SLC v4.0 and later:** This is the number of bytes the SLC device port receives before it forwards them to the SLM. For example, a threshold preset at 128 characters means that as soon as the SLC receives 128 bytes of data on this particular device port, it captures log data and sends the received data regarding this device port to the SLM. The minimum byte threshold is **1**, and the default is **1024**.
Break Sequence	A series of one to ten characters users can enter on the command line interface to send a break signal to the external device. A suggested value is **Esc+B** (escape key, then uppercase "B" performed quickly but not simultaneously). You would specify this value as **\x1bB**, which is hexadecimal **(\x)** character 27 (**1B**) followed by a **B**.
Managed Device	Not active when you are adding a port.

Data Settings

Baud	The speed with which the device port exchanges data with the attached serial device. From the drop-down list, select the baud rate. Most devices use 9600 for the administration port, so the device port defaults to this value. Check the equipment settings and documentation for the proper baud rate.
Data Bits	Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is **8** data bits.
Stop Bits	The number of stop bit(s) used to indicate that a byte of data has been transmitted. From the drop-down list, select the number of stop bits. The default is **1**.
Parity	Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is **none**.
Flow Control	A method of preventing buffer overflow and loss of data. The available methods include none, xon/xoff (software), and RTS/CTS (hardware). The default is **none**.
Enable Logins	For serial devices connected to the device port, displays a login prompt and authenticates users. Successfully authenticated users are logged into the command line interface. Disabled is the default and is the correct setting if the device port is the endpoint for a connection.

Hardware Signal Triggers

Check DSR on Connect	If this setting is enabled, the device port only establishes a connection if DSR (Data Set Ready) is in an asserted state. DSR should already be in an asserted state, not transitioning to, when a connection attempt is made. Disabled by default unless dial-in, dial-out, or dial-back is enabled for the device port.

Disconnect on DSR	If a connection to a device port is currently in session, and the DSR signal transitions to a de-asserted state, the connection disconnects immediately. Disabled is the default unless dial-in, dial-out, or dial-back is enabled for the device port.

IP Settings

Enable Telnet In	Enables access to this port through Telnet. Disabled by default.
Enable SSH In	Enables access to this port through SSH. Disabled by default.
Enable TCP in	Enables access to this port through a raw TCP connection. Disabled by default. ***Note:*** *When using raw TCP connections to transmit binary data, or where the break command (escape sequence) is not required, clear the* ***Break Sequence*** *of the respective device port.*
Port	Automatically assigned Telnet, SSH, and TCP port numbers. You may override this value, if desired.
Authenticate	If selected, the SLM requires user authentication before granting access to the port.

3. Click the **Add** button. A confirmation message displays, and the port is now listed below the Ethernet device on the menu tree.

Updating or Deleting a Port

Administrators and permitted Ethernet Device Account groups can update or delete a port.

To delete a port:

1. On the device's **Ports** tab, click the **Edit** icon to the left of the port name,

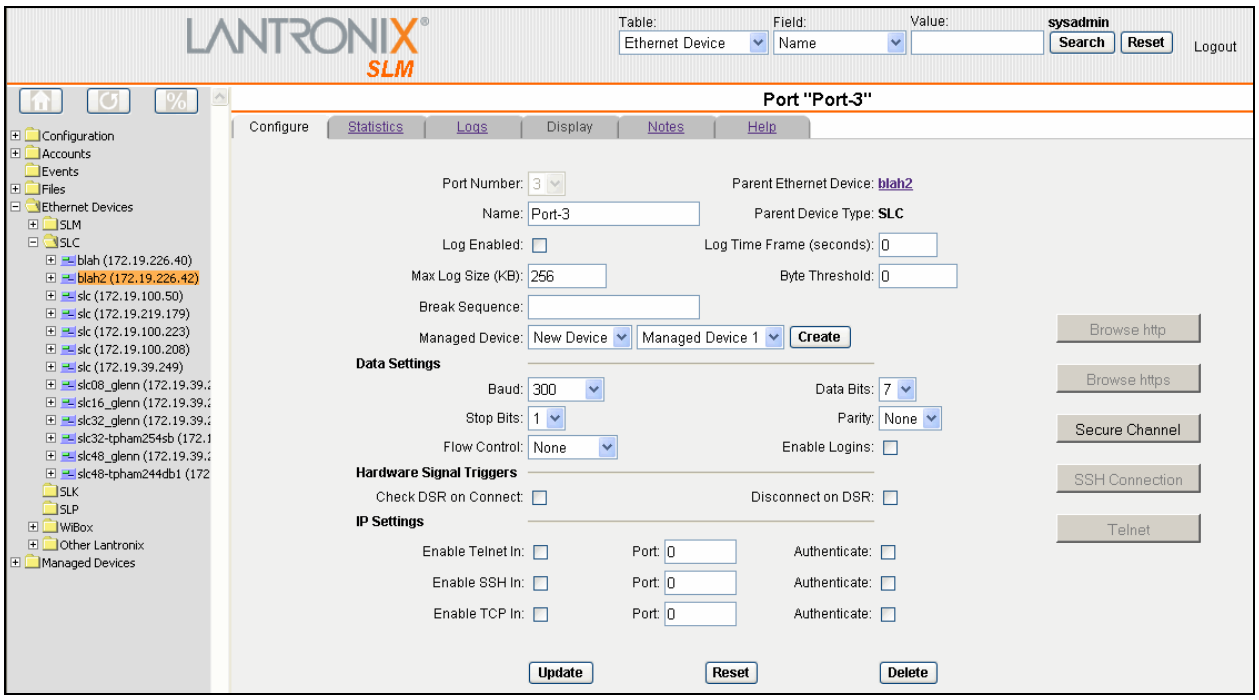
   OR

   On the device's menu tree, select the port.

   The following page opens:

Figure 8-24. Port Page – Configure Tab

Note: The page below shows and SLC port. Devices other than the SLC do not display as much information.



2. Click the **Delete** button.
3. In response to the request for confirmation, click **OK**. A message confirming the deletion displays.

   The deleted port is no longer listed on the Ethernet device's menu tree or on the device's **Ports** tab.

To update a port:

1. Add or update information as desired. In addition to the fields completed when adding a port, complete the following fields:

Managed Device	If desired, create a managed device from the port. (See *Creating Individual Managed Devices* on page 164.) *Note: This field is unavailable if no Managed Device Groups exist in the system.*
TCP Port for Terminal (SCS and SLP)	Port number to use when establishing a Telnet connection via that port. A value of zero means use the default port (which is 23); otherwise use the entered value.

2. Click the **Update** button. When the update is complete, a confirmation message displays.

Note: Port configuration fields differ depending on the parent device type.

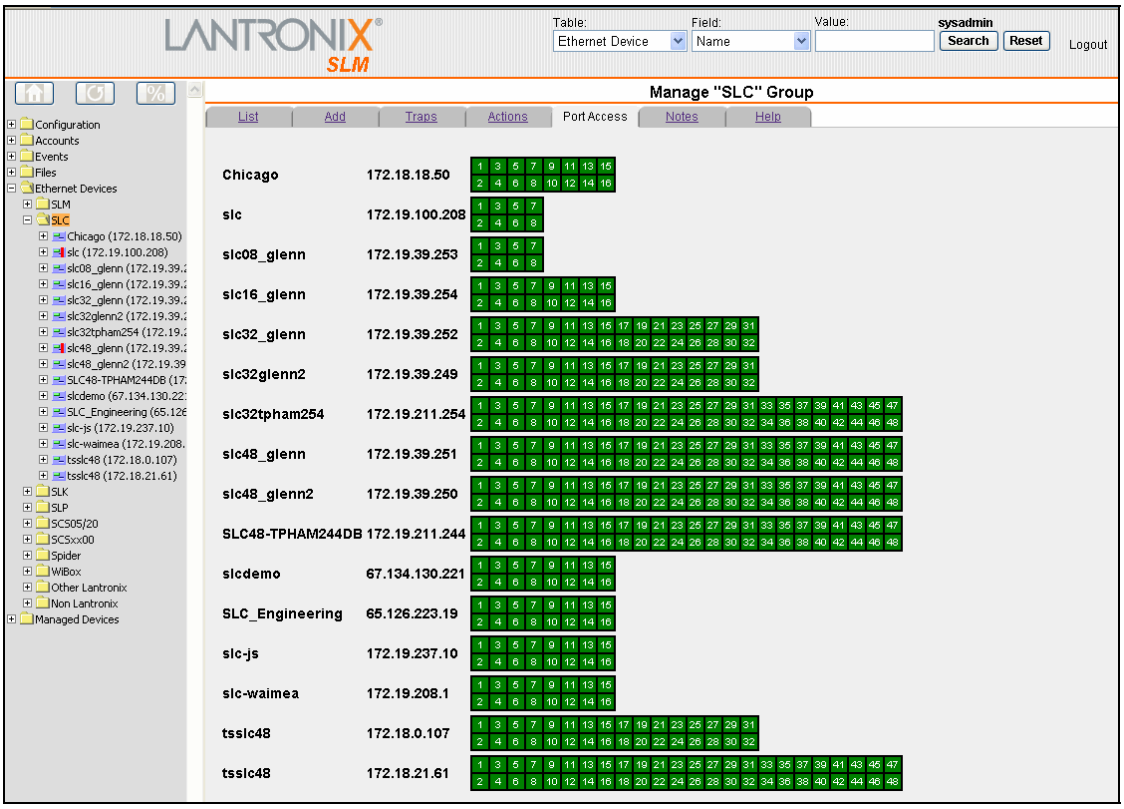
Connecting Directly to the Port of an SLC or BOB

You can get quick secure channel access to any port on any SLC (or BOB).

To gain quick secure channel access to an SLC port:

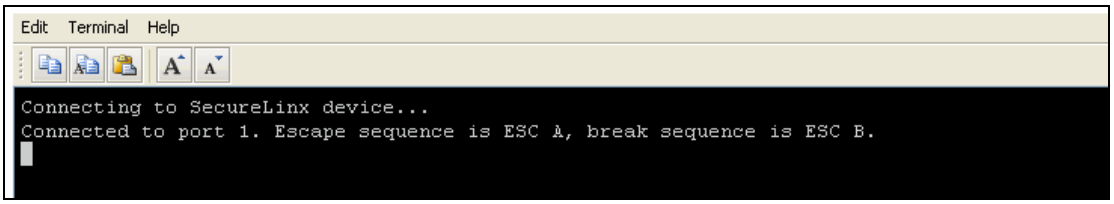
1. On the Manage SLC Group page, click the **Port Access** tab. The following page displays:

Figure 8-25. Manage SLC Group Page – Port Access Page



2. Click the desired port on the specific SLC. The following page displays:

Figure 8-26. Connection to Selected SLC Port



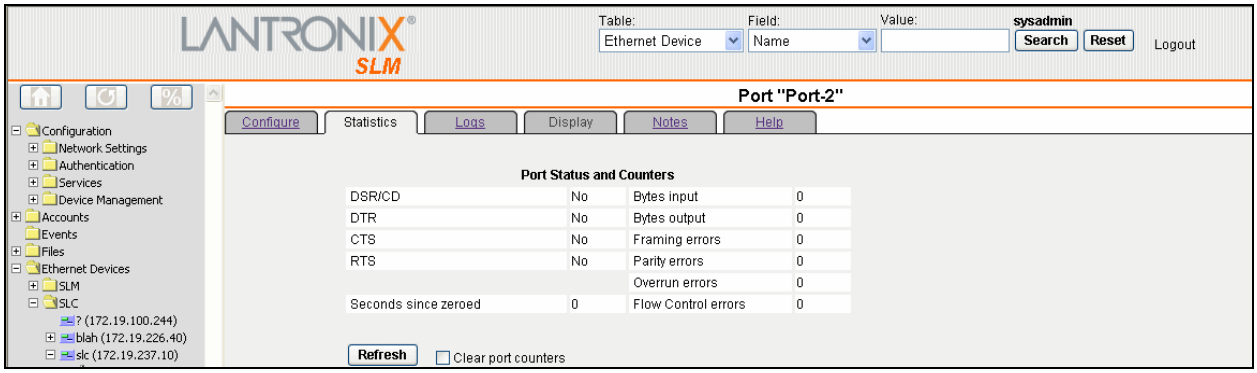
Statistics

Users authorized to view or interact with the port may view status and statistics about it.

To view port status and statistics:

1. On the **Port** page, click the **Statistics** tab. The following page opens:

Figure 8-27. Port Page -- Statistics Tab



The page displays port status and counters.

2. To see the current statistics, click the **Refresh** button.
3. To clear the port counters, select the **Clear** port counters check box and click the **Refresh** button.

Applying Power to SLP Ports on a Single Device

You can power on, power off, or cycle power on multiple ports on an SLP.

To manage power on multiple ports of an SLP:

1. On the SLP's Device page, click the **Ports** tab. The following page opens:

Figure 8-28. SLP's Device Page -- Ports Tab

2. Select the ports whose power you want to power on, power off, or cycle.
3. From the drop-down list at the bottom of the page, select the action you want to take (**Power On**, **Power Off**, or **Cycle Power**).
4. Click the **Update** button.

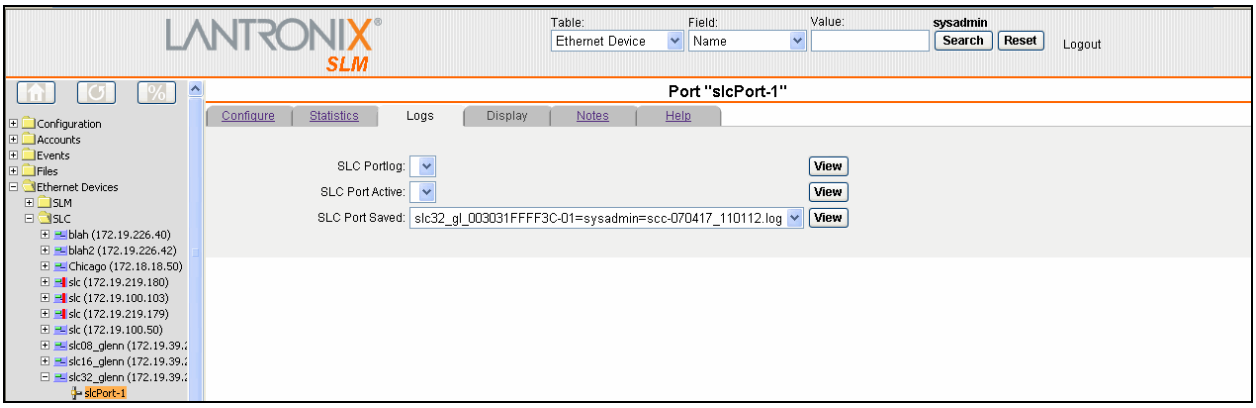
Viewing Port Logs

Depending on the type of device, you can view one or more port and session logs on the Port page.

To view logs:

1. On the Port page, click the **Logs** tab. The following page displays:

Figure 8-29. Port Page – Logs Tab



2. To view a log, select the log from the appropriate drop-down list:

Note: *The SLC enables you to view three types of logs, while other devices enable you to view only the current session.*

SLC Portlog	Select the log of this particular SLC device port.
SLC Port Active	Select the log of a currently active SLM user session to the port.
SLC Port Saved	Select a session log of a saved SLM user session to the port.

3. Click the **View** button. The log displays on the **Display** tab.

Port Commands

`set ethernetdevice port`

Syntax

```
set ethernetdevice port <Device Name or IP Address> portnumber
<Port Number> <one or more parameters>
```

Parameters

`[name <Port Name>]`

`[<on|off|cyclepower>]` (available for SLP only)
Powers Ethernet device port on or off.

Example

To power up SLP outlet 2:

```
set eth port slp-sunset po 2 state on
```

Description

Finds a port by device name or IP address along with the port number and modifies port parameters.

show ethernetdevice port

Syntax

```
show ethernetdevice port <Device Name or IP Address> all
```

```
show ethernetdevice port <Device Name or IP Address> portnumber <Port Number>
```

Description

Finds an Ethernet device using device name or IP address and displays port information.

show ethernetdevice search port

Syntax

```
show ethernetdevice search port <one or more parameters>
```

Parameters

Note: *Search entries are not case sensitive.*

```
[name <Port Name>]
```

```
[portnumber <Port Number>]
```

Examples

```
show ethernetdevice search port name waimea-port
```

```
show ethernetdevice search port name waimea portnumber 2
```

Description

Displays all ports that match the criteria entered.

show port

Syntax

```
show port <name>
```

Type `show port all` to display index.

Example

`show port slc` displays all Ethernet ports whose name starts with "slc."

Description

Searches Ethernet ports by port name and displays port information.

show port all

Syntax

```
show port all
```

```
show port
```

Displays all Ethernet ports.

show port index

Note: *Type* `show port all` *to display index.*

Syntax

```
show port index <number>
```

Description

Displays Ethernet ports by index.

9: Managed Devices

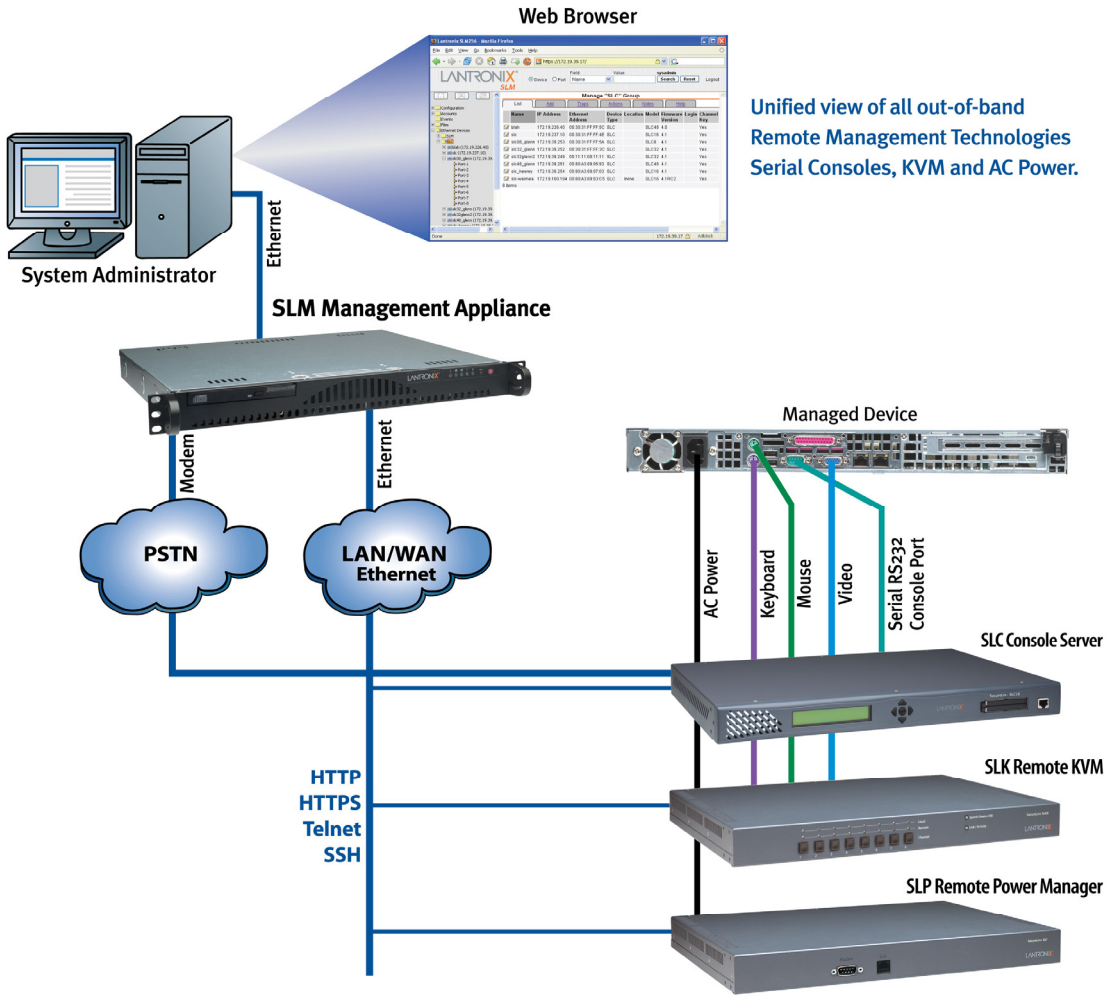
SLM v2.2 can treat any device connected to a port or connected to the local network as a *managed device*. Furthermore, multiple managed device objects in the system may be *fused* into a single managed device to streamline managed device operations and access.

For example, a single device (e.g., a UNIX server) may be connected to an SLC by a serial port, to an SLP by a power connector, and to an SLK by a KVM port. You could manage these three individual managed devices separately. However, if you fuse the individual managed devices into one virtual managed device, you can then manage the SLC, SLP, and SLK connections from a single SLM web page.

Each virtual managed device in the SLM system can include a connection to:

- 1 SLC serial port
- 1 SLK KVM port
- 2 SLP power ports
- 1 local Ethernet device

Figure 9-1. Virtual Managed Device



To create individual managed devices and fuse individual devices into a virtual managed device, you have the following options:

On the Port or Device Page: Create a new managed device or fuse a new managed device into an existing managed device.

On the Ports Page: Create one or more managed devices at the same time.

On the Managed Device Group Page: Select two or more individual managed devices and fuse them to create a virtual managed device.

Managed Device Groups

Managed devices are assigned to Managed Device Groups so that users can easily locate them.

Administrators, authorized Ethernet Device Account group users, and authorized Managed Device Account Group users can organize the devices attached to Ethernet ports into groups. For example, an administrator may want to create groups by location, type of device, or user. A Managed Device Group may include devices attached to the ports of several different Ethernet devices.

The administrator creates custom groups of managed devices and then assigns individual devices to the groups. For example, a group called Lab 1 might include all devices attached to the ports of Ethernet devices being tested. The administrator and permitted users can delete a Managed Device Group.

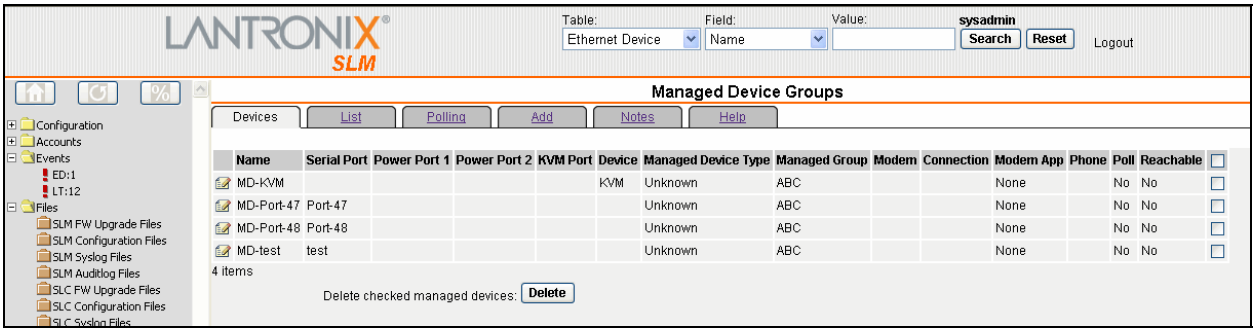
Viewing All Managed Devices

You can view a list all managed devices in the system.

To view all managed devices:

1. On the menu, click **Managed Devices**. The **Devices** tab on the Managed Device Groups page opens.

Figure 9-2. Managed Device Groups Page – Devices Tab



2. View the following information about each managed device:

Name	Name of the managed device.
Serial Port	Name of an SLC or SCS serial port that is connected to this managed device.
Power Port 1	Name of an SLP power port that is connected to this managed device.
Power Port 2	Name of an SLP power port that is connected to this managed device.
KVM Port	Name of an SLK port that is connected to this managed device.
Device	Name of a local Ethernet device.
Managed Device Type	Type of managed device (e.g., Solaris Server or Linux Server). ***Note:*** *If the managed device type is set to Windows, a* ***Remote Desktop*** *option becomes available.*

Managed Group	Name of the Managed Device Group to which the managed device belongs.
Modem	Name of the modem to be used when connecting to the managed device.
Connection	Name of the connection to be used with modem access.
Modem App	Application to invoke for the connection (e.g., Secure Channel, SSH, Telnet).
Phone	Telephone number of the modem on the managed device.
Poll	Indicates whether to check the managed device for modem connectivity during modem polling testing.
Reachable	Indicates whether a connection to the modem on this managed device was successful the last time it was tested.

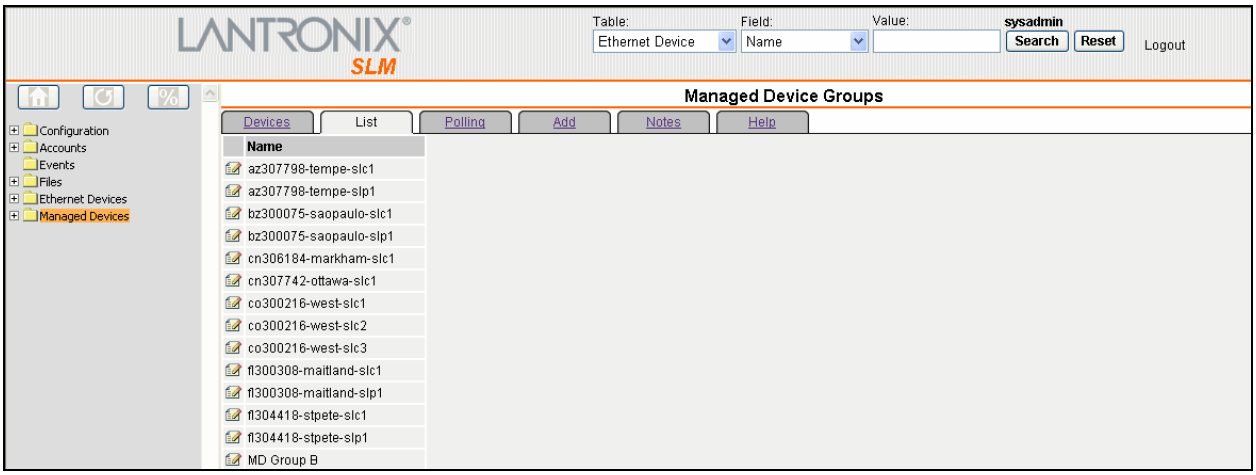
Viewing Managed Device Groups

You can view a list of all the Managed Device Groups and view devices by group.

To view a list of Managed Device Groups:

1. On the menu, click **Managed Devices**, and then click the **List** tab. The following page opens:

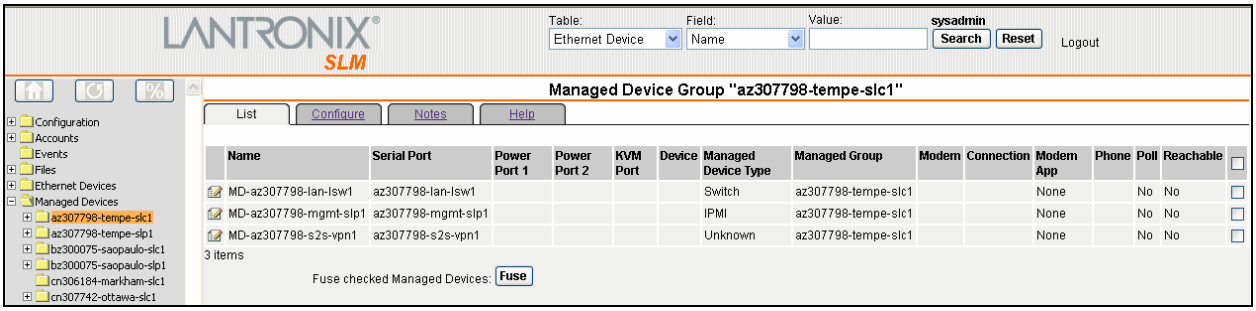
Figure 9-3. Managed Device Groups Page – List Tab



To view a list of devices belonging to a Managed Device Group:

1. On the menu tree, click the name of the device group. The following page opens:

Figure 9-4. Managed Device Group Page – List Tab



2. View the information about each device:

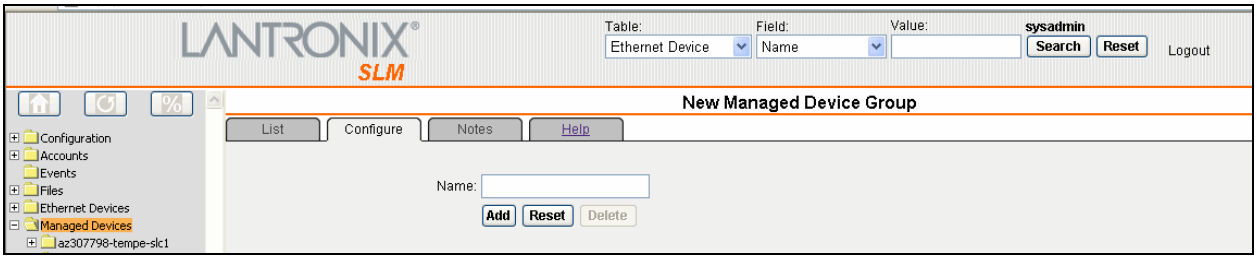
Adding a Managed Device Group

The administrator creates custom groups of managed devices and then assigns individual devices to the groups. For example, a group might include all devices attached to the ports of Ethernet devices being tested.

To add a Managed Device Group:

1. On the menu, click **Managed Devices**, and then click the **Add** tab. The following page opens:

Figure 9-5. New Managed Device Group Page – Configure Tab



2. In the **Name** field, enter the name of the Managed Device Group.
3. Click the **Add** button.
4. Expand **Managed Devices** on the menu tree. The custom group displays as a folder.

Note: *A managed device may belong to only one Managed Device Group.*

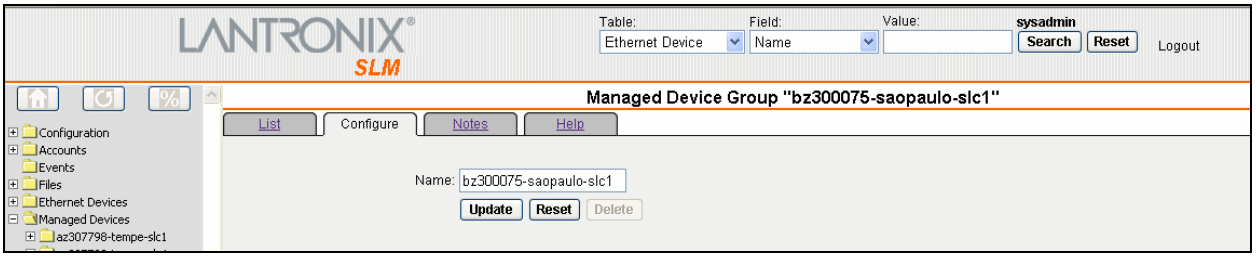
Updating or Deleting a Managed Device Group

The administrator can update or delete a Managed Device Group.

To update or delete a Managed Device Group:

1. On the menu, click the Managed Device Group. The following page opens:

Figure 9-6. Managed Device Group Page – Configure Tab



To update a Managed Device Group:

1. Change the name of the group and click the **Update** button. A confirmation message displays.

To remove the Managed Device Group:

Note: *You can only delete a Managed Device Group that has no devices assigned to it*

1. Click the **Delete** button.
2. In response to the confirmation request, click **OK**. A message confirming the deletion displays. The menu no longer displays the Managed Device Group.

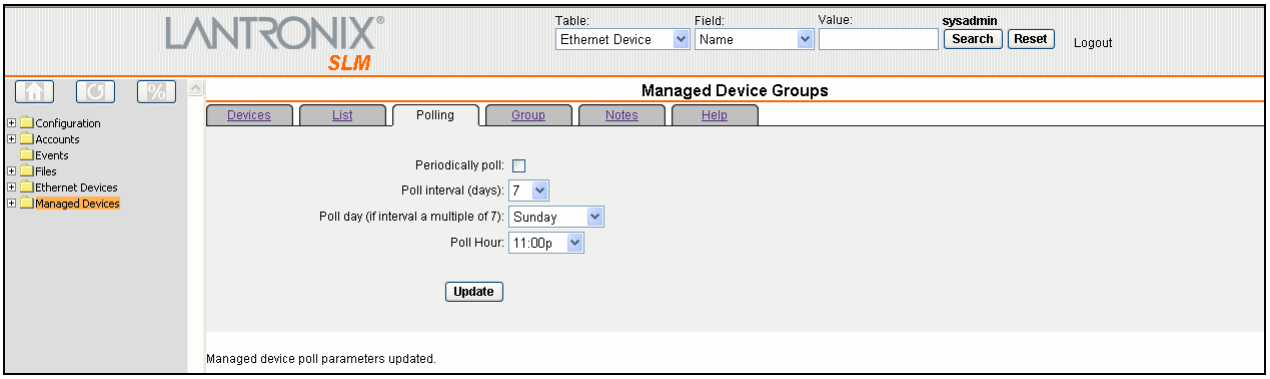
Configuring Polling Settings

The system administrator or permitted user can specify polling settings for the Managed Device Group. The SLM polls the Managed Device Group's connections according to these settings.

To configure polling settings:

1. On the menu, click **Managed Devices**, and then click the **Polling** tab. The following page opens:

Figure 9-7. Managed Device Groups – Polling Tab



2. Enter the following information:

Periodically poll	Select the check box to enable periodic polling of the Managed Device Group's connections. Disabled by default.
Poll interval (days)	From the drop-down list, select the number of days between polls. The range is between 1 and 30. The default is **7**.
Poll day (if interval a multiple of 7)	If the poll interval is a multiple of **7**, from the drop-down list, select the day of the week on which the SLM should poll the connections.
Poll Hour	Enter the time of day at which the SLM should poll the connections.

3. To save the settings, click the **Update** button.

Managed Device Group Commands

show manageddevice all

Syntax

```
show manageddevice all
show manageddevice
```

Description

Displays information about all managed devices.

show manageddevice group

Syntax

```
show manageddevice group <Group Name> group name
```

Description

Displays all managed devices by Managed Device Group.

show manageddevice groupnames

Syntax

```
show manageddevice groupnames
```

Description

Displays all Managed Device Group names

Connecting to a Managed Device

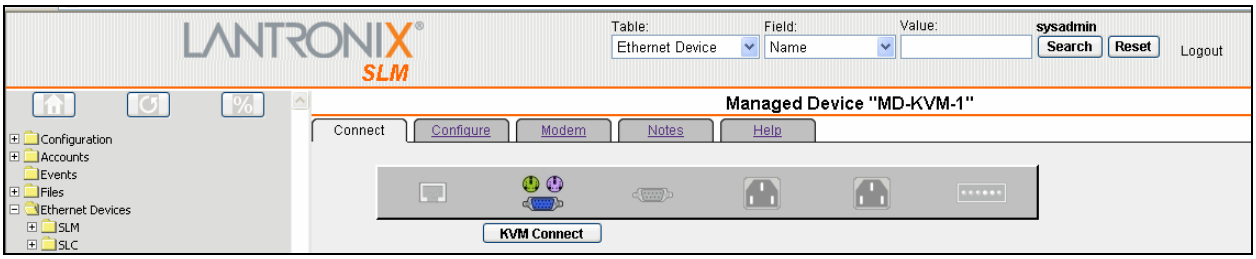
The **Connect** tab on the Managed Device page provides various methods of connecting directly to a managed device. The method depends on the type of Lantronix device server or modem connected to the managed device. The ability to connect also depends on the user's permissions.

To view connection methods to a managed device:

1. On the menu, select the managed device. The following page opens:

   Note: *This example shows a connection to a KVM port.*

Figure 9-8. Managed Device Page -- Connect Tab



An icon bar contains a series of icons representing the types of connections the SLM can make to managed devices. Buttons above or below the icons enable you to connect directly to the managed device. Icons for options not configured into the device are unavailable.

In the example above, the button below the **SLK** icon enables you to connect to the managed device through a KVM port on an SLK.

Note: *For more information about connection methods, see* Connecting to Ethernet and Managed Devices *on page 187.*

Table 9-1. Connection Icons and Buttons on the Connect Tab

Icon	Connection Buttons	Description
	HTTP HTTPS Web Channel Secure Channel SSH Connection Telnet	**Network connection:** Enables the SLM to connect to a managed device directly by means of HTTPS, Secure Channel, Web Channel, SSH Connection, or Telnet. ***Note:*** *If the managed device incorporates a local Ethernet device, and that device type is set to Windows, then a* ***Remote Desktop*** *button displays. If the managed device type is set to Linux Server, a* ***VNC*** *button displays.*
	KVM HTTP KVM HTTPS	**KVM HTTP connection:** Enables the SLM to connect to the managed device through a port on an SLK using a nonsecure web connection. **KVM HTTPs connection:** Enables the SLM to connect to the managed device through a port on an SLK using a secure web connection.

Icon	Connection Buttons	Description
	Start Logging Secure Channel	**SLC Serial Connection:** Enables the SLM to connect to the managed device through an SLC serial port by secure channel and to cause the managed device to start logging to an SLC. SLCs display the **Secure Channel** button. SCSs as well as Other Lantronix and Non-Lantronix devices display the **SSH Connection** button for the serial port. ***Note:*** *If logging is on, the **Stop Logging** button displays instead of the **Start Logging** button, and vice versa.*
	Cycle Power Power On Power Off	**Power connection:** Enables the SLM to control power on the managed device through an SLP port. Two power connections are available. ***Note:*** *If the SLM detects that the power is on, then only the **Power Off** and **Cycle Power** buttons display. If the SLM detects that the power is off, only the Power **On** button displays. If the state of the power connection is not known, all buttons display (but you also get a message letting you know that the state was not detectable).*
	Connect	**Modem:** Enables the SLM to connect to the managed device through the telephone network. ***Note:*** *This button reads **Connect** when no session has been established and during session negotiation. Refresh the page after establishing a session, and this button reads **Disconnect**. If you click the **Disconnect** button, be sure to refresh the page as the session may not have terminated when the new page was rendered.*

2. To identify the port or device on the device server to which the managed device is connected, move the pointer over the icon.
3. To go directly to the port or device page, click the icon.

Creating Individual Managed Devices

The administrator and permitted users can create individual managed devices in the following ways:

- From a port
- From a list of ports
- From a device

From a Port

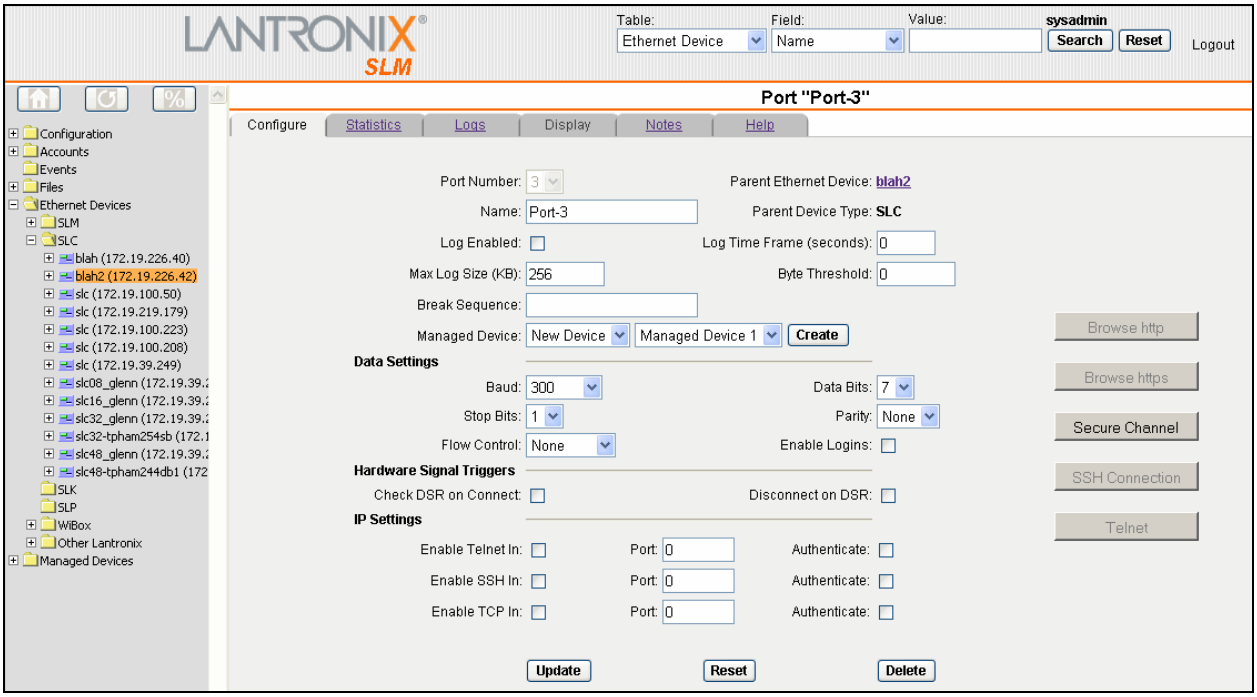
You can create a managed device from a port on a Lantronix device server such as an SLC, SLK, SLP, SCS05/20, or SCSxx00. The managed device represents the physical device connected to the port.

To create a managed device from a port:

1. On the menu, click the icon for a port that belongs to an Ethernet device. The Port page opens.

   Note: *In this example, we show a port on an SLC.*

Figure 9-9. Port Page – Configure Tab



2. Leave **New Device** in the **Managed Device** drop-down list, and select the Managed Device Group to which the new device will belong.
3. Click the **Create** button.

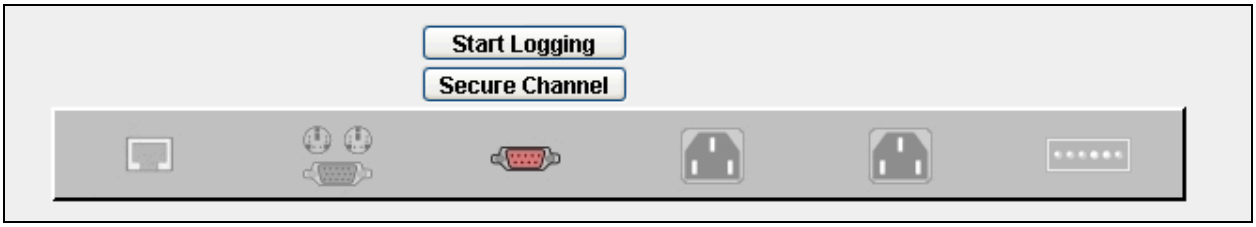
   The managed device field displays as a link to the managed device's configuration page, and the menu tree lists the new managed device in the assigned Managed Device Group.

   A **Defuse** button displays to the right of the link. Click the button to remove this port from the managed device. If the port was the only component of the managed device, the **Defuse** button removes the managed device itself from the system.

Figure 9-10. Link to a Managed Device Page – Configure Tab

4. On the menu, click the name of the new managed device. The Managed Device page **Connect** tab displays the available connection buttons for the serial connection.

Figure 9-11. Managed Device Page – Connect Tab



In a similar manner, you can create individual managed devices from SLP ports and SLK connectors.

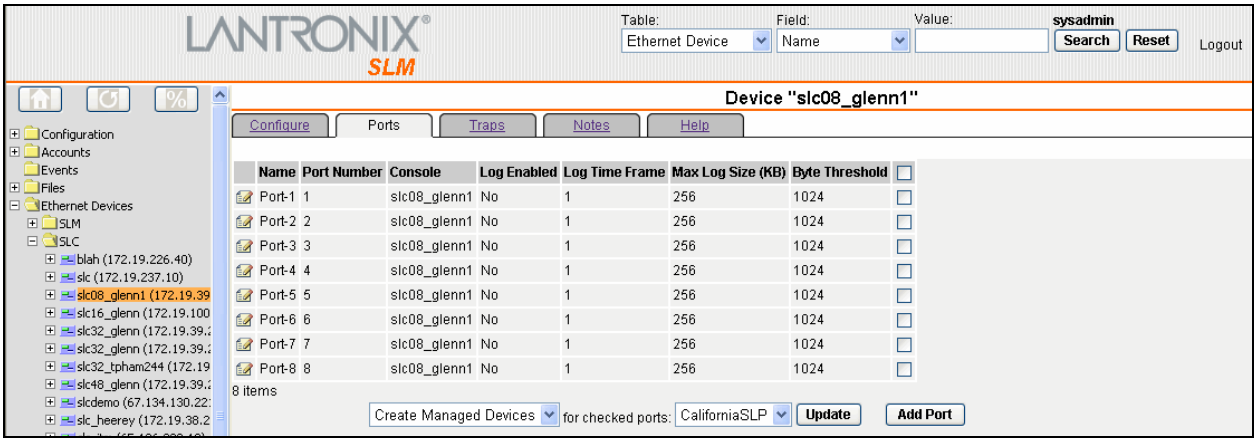
From a Ports List

You can create one or more managed devices from an Ethernet device's ports list. In this example, we show ports on an SLC.

To create one or more managed devices on the Ports page:

1. On the Device page, click the **Ports** tab. The following page opens:

Figure 9-12. Device Page - Ports Tab



2. Select the check box for one or more ports on the SLC that will be connected to serial devices.
3. From the drop-down list box at the bottom of the page, select **Create Managed Devices**.
4. From the **for checked ports** drop-down list box, select the Managed Device Group to which the selected managed device(s) will belong.
5. Click the **Update** button.
6. In response to the confirmation request, click **OK**. The menu tree displays the new managed device(s) in the assigned Managed Device Group.
7. If desired, repeat steps 2-6 above to create managed devices and assign them to other Managed Device Groups.

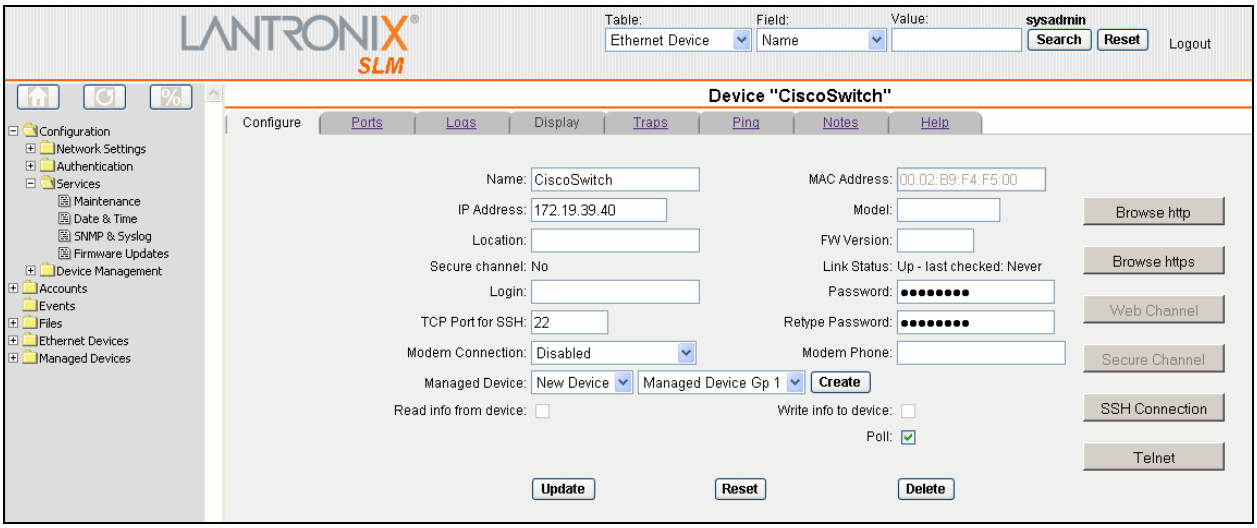
From an Ethernet Device

Administrators and permitted users can create a managed device from any auto-discovered or manually added Ethernet device, such as a server or a switch, and assign it to a Managed Device Group.

To create a managed device from an Ethernet device:

1. On the menu, click the name of the device (in this example, a Cisco switch). The following page opens:

Figure 9-13. Device Page for Cisco Switch



2. In **Managed Device**, leave **New Device** and from the **Group** drop-down list, select the Managed Device Group to which the new managed device will belong.
3. Click the **Create** button.

   When the page redisplays, the **Managed Device** field displays as a link to the new managed device, and the assigned Managed Device Group in the menu lists the new managed device.

   A **Defuse** button displays to the right of the link. Click the button to remove this device from the managed device. If the device was the only component of the managed device, the **Defuse** button removes the managed device itself from the system.
4. To view the **Connect** tab for the managed device, click the name of the managed device on the menu. Above the network icon are four buttons for connecting to the device through the network.

Note: *For more information about connection methods, see* *Connecting to Ethernet and Managed Devices on page 187.*

Fusing Managed Devices

While the SLM can communicate with a device connected to a port of a Lantronix device server (e.g., an SLC, SLK, or SCS05/2) individually, it is often more convenient to communicate from a single web page to a *virtual* managed device composed of more than one connection to the device. The process of creating the virtual managed device from individual managed devices is called *fusing*. One convenient application is to fuse the SLC, SLK, and SLP port connections that manage a single Ethernet device such as a server or a switch.

Methods of Fusing

There are two methods of fusing individual managed devices together:

- On the Port or Device page, fuse a new managed device with an existing one.
- On the Managed Device Group page, fuse several existing managed devices at once.

Guidelines

Follow the guidelines below when fusing managed devices:

- The managed devices must be in the same Managed Device Group.
- A virtual managed device can consist of only one device (local), one SLC port, one SLK port, two SLP ports, and one modem.

Fusing a Port with an Existing Managed Device

The Port Configure tab provides an opportunity to merge a single port with an existing managed device. Previously, we showed an example of creating a managed device from an SLC port.

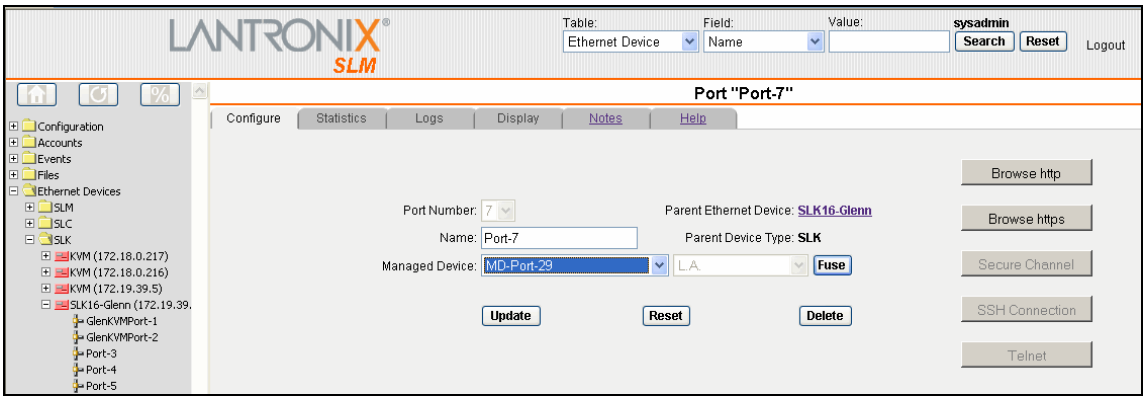
In the following example, as we configure an SLK port, we fuse it with the SLC port managed device.

To fuse a port with an existing managed device:

1. On the menu tree of an Ethernet device such as an SLC or SLK, select the port.

   The following page opens:

Figure 9-14. Fusing on a Port Page – Configure Tab



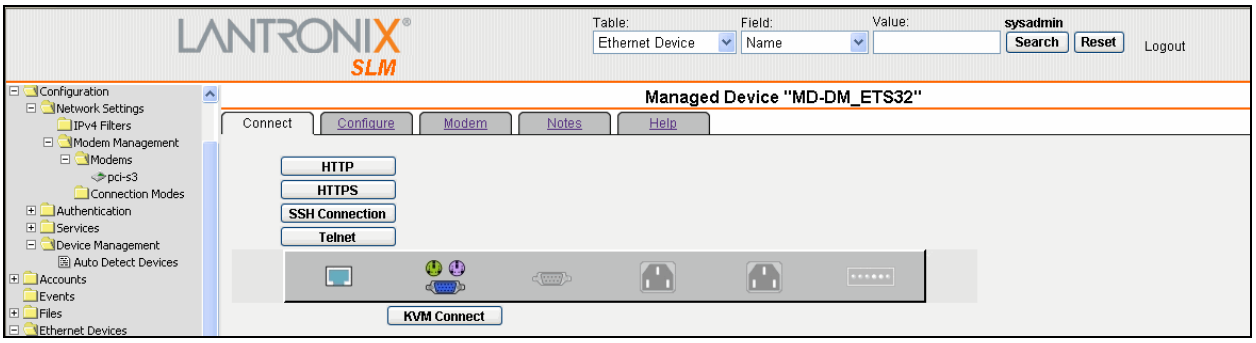
2. From the **Managed Device** drop-down list, select the existing managed device.
3. Click the **Fuse** button (changed from the **Create** button).

The Managed Device field now displays as a link to the virtual managed device, which has the name of the original managed device.

A **Defuse** button displays to the right of the link. Click the button to remove this port from the managed device. If the port was the only component of the managed device, the **Defuse** button removes the managed device itself from the system.

4. To view the **Connect** tab, click the name of the virtual managed device in the menu.

Figure 9-15. Virtual Managed Device Page with Two Connections



There are four connection buttons above the Ethernet icon and one below the KVM icon , enabling you to connect to the physical managed device through the network and the SLK connection.

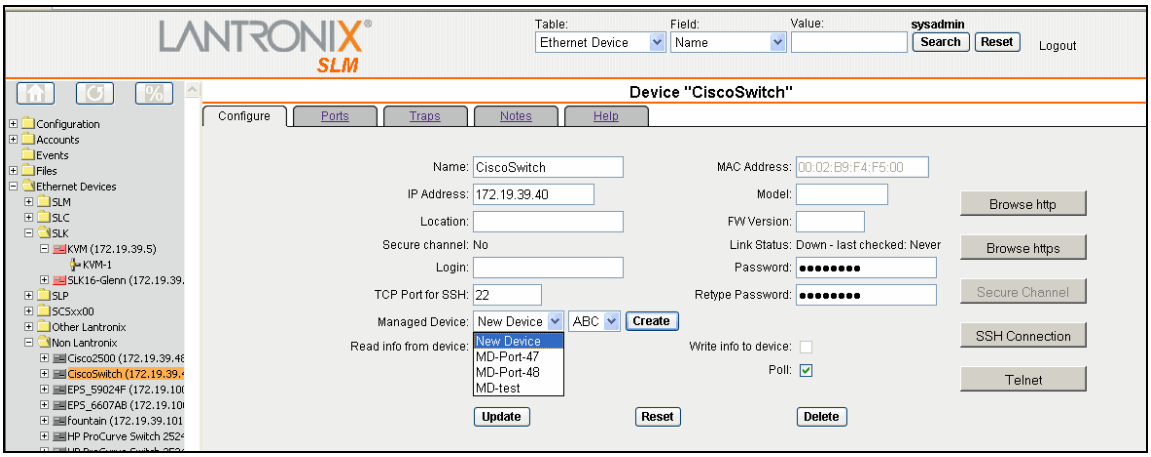
Fusing an Ethernet Device with an Existing Managed Device

The physical device to which a Lantronix device server or a modem is connected may be fused with an existing managed device.

To fuse a device with an existing managed device:

1. On the menu, click the name of the Ethernet device. In this example, we use a switch.

Figure 9-16. Fusing a Managed Device on the Device Page



2. From the **Managed Device** drop-down list, select the existing managed device.
3. Click the **Fuse** button (changed from the **Create** button).

   The Managed Device field now displays as a link to the virtual managed device, which has the name of the original managed device. The virtual managed device

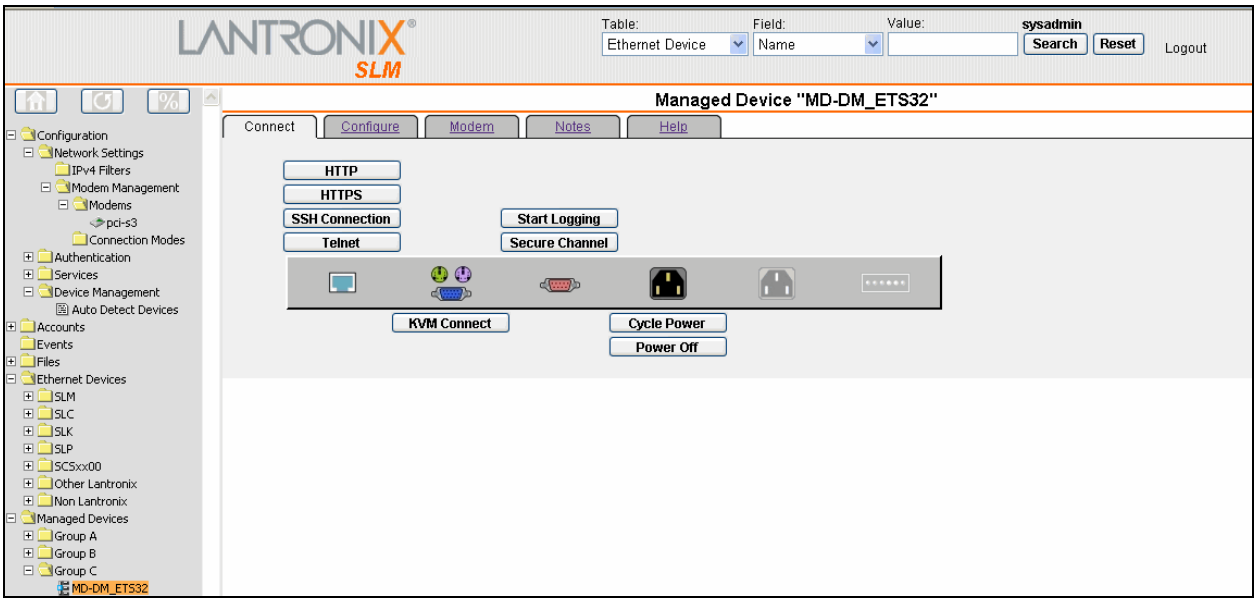
has taken the name of the existing managed device and still displays in the Managed Device Group.

A **Defuse** button displays to the right of the link. Click the button to remove this device from the managed device. If the device was the only component of the managed device, the **Defuse** button removes the managed device itself from the system.

Continuing the One-at-a-Time Fusion Process

If you continue in this manner, fusing a new serial port managed device and then a new power managed device into the original managed device in the examples above, the **Connect** tab would look like this:

Figure 9-17. Virtual Managed Device on Managed Device Page – Connect Tab



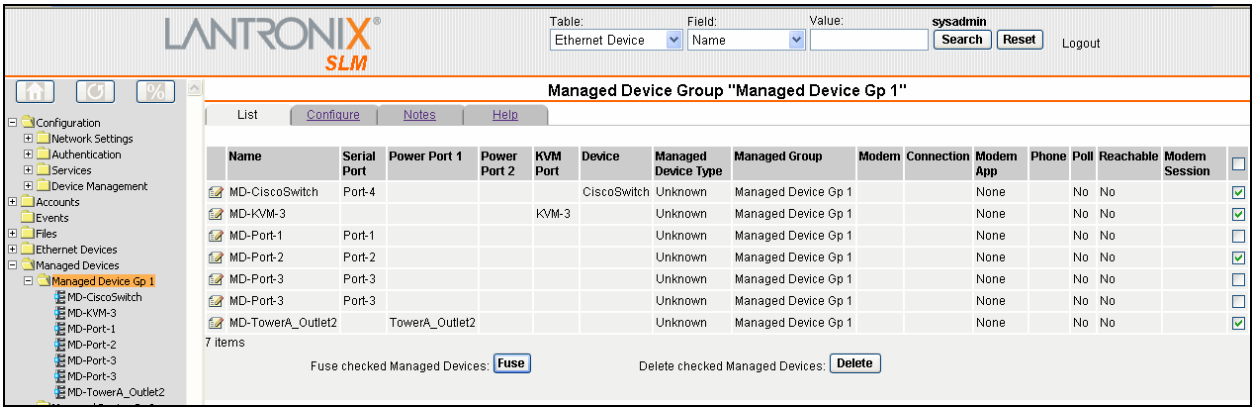
Fusing Managed Devices on the Managed Device Group Page

Another place to fuse individual managed devices is on the Managed Device Group page. Here you use a single web page to fuse multiple managed devices at the same time.

To use the Managed Device Group page to fuse managed devices:

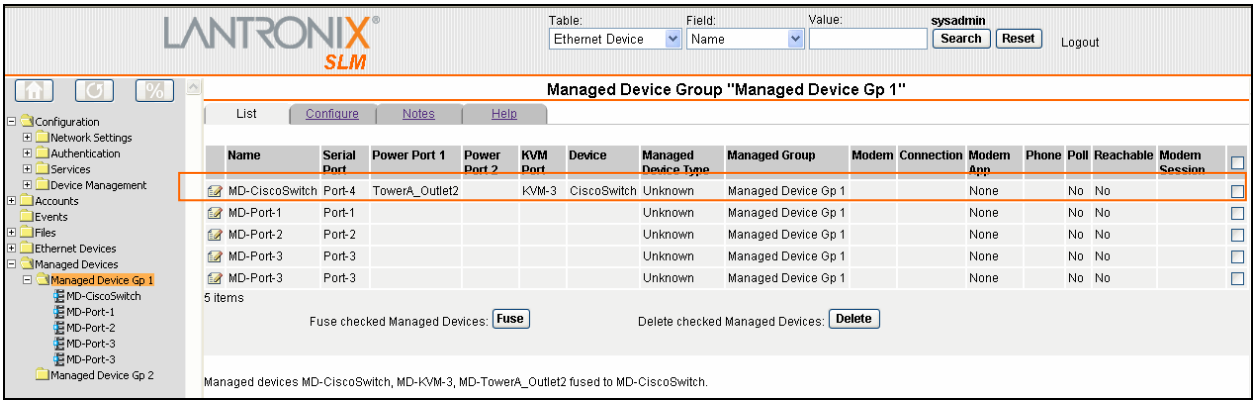
1. On the menu, click the name of the Managed Device Group that includes the managed devices you want to fuse. This page that opens displays a table listing all the managed devices within the group.

Figure 9-18. Managed Device Group – List Tab


LANTRONIX SLM
Table: Ethernet Device
Field: Name
Value:
sysadmin
Search
Reset
Logout
Managed Device Group "Managed Device Gp 1"
List
Configure
Notes
Help
Name | Serial Port | Power Port 1 | Power Port 2 | KVM Port | Device | Managed Device Type | Managed Group | Modem | Connection | Modem App | Phone | Poll | Reachable | Modem Session
MD-CiscoSwitch | Port-4 | | | | CiscoSwitch | Unknown | Managed Device Gp 1 | | | None | | No | No |
MD-KVM-3 | | | | KVM-3 | | Unknown | Managed Device Gp 1 | | | None | | No | No |
MD-Port-1 | Port-1 | | | | | Unknown | Managed Device Gp 1 | | | None | | No | No |
MD-Port-2 | Port-2 | | | | | Unknown | Managed Device Gp 1 | | | None | | No | No |
MD-Port-3 | Port-3 | | | | | Unknown | Managed Device Gp 1 | | | None | | No | No |
MD-Port-3 | Port-3 | | | | | Unknown | Managed Device Gp 1 | | | None | | No | No |
MD-TowerA_Outlet2 | | TowerA_Outlet2 | | | | Unknown | Managed Device Gp 1 | | | None | | No | No |
7 items
Fuse checked Managed Devices: Fuse
Delete checked Managed Devices: Delete
Configuration
Network Settings
Authentication
Services
Device Management
Accounts
Events
Files
Ethernet Devices
Managed Devices
Managed Device Gp 1
MD-CiscoSwitch
MD-KVM-3
MD-Port-1
MD-Port-2
MD-Port-3
MD-Port-3
MD-TowerA_Outlet2

2. Select the check box for each managed device you want to fuse.
3. Click the **Fuse** button.
4. In response to the confirmation request, click **OK**. The page redisplays:

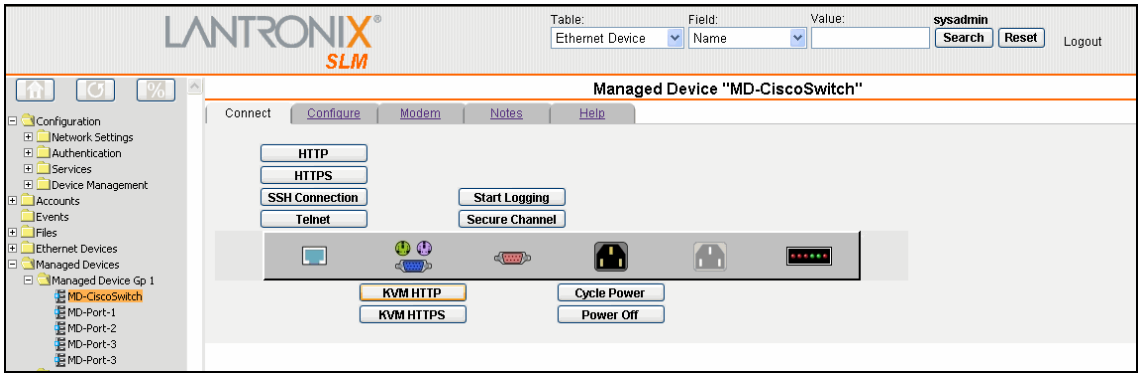
Figure 9-19. Managed Device Group Page – List Tab (After Fusion)


LANTRONIX SLM
Table: Ethernet Device
Field: Name
Value:
sysadmin
Search
Reset
Logout
Managed Device Group "Managed Device Gp 1"
List
Configure
Notes
Help
Name | Serial Port | Power Port 1 | Power Port 2 | KVM Port | Device | Managed Device Type | Managed Group | Modem | Connection | Modem App | Phone | Poll | Reachable | Modem Session
MD-CiscoSwitch | Port-4 | TowerA_Outlet2 | | KVM-3 | CiscoSwitch | Unknown | Managed Device Gp 1 | | | None | | No | No |
MD-Port-1 | Port-1 | | | | | Unknown | Managed Device Gp 1 | | | None | | No | No |
MD-Port-2 | Port-2 | | | | | Unknown | Managed Device Gp 1 | | | None | | No | No |
MD-Port-3 | Port-3 | | | | | Unknown | Managed Device Gp 1 | | | None | | No | No |
MD-Port-3 | Port-3 | | | | | Unknown | Managed Device Gp 1 | | | None | | No | No |
5 items
Fuse checked Managed Devices: Fuse
Delete checked Managed Devices: Delete
Managed devices MD-CiscoSwitch, MD-KVM-3, MD-TowerA_Outlet2 fused to MD-CiscoSwitch.
Configuration
Network Settings
Authentication
Services
Device Management
Accounts
Events
Files
Ethernet Devices
Managed Devices
Managed Device Gp 1
MD-CiscoSwitch
MD-Port-1
MD-Port-2
MD-Port-3
MD-Port-3
Managed Device Gp 2

The components of the virtual managed device now display on the same row, and a message in the message area confirms the fusion. The virtual managed device takes the name of the individual managed device that was in the highest row. In the Managed Device Group on the menu, that name remains, but the other fused components do not.

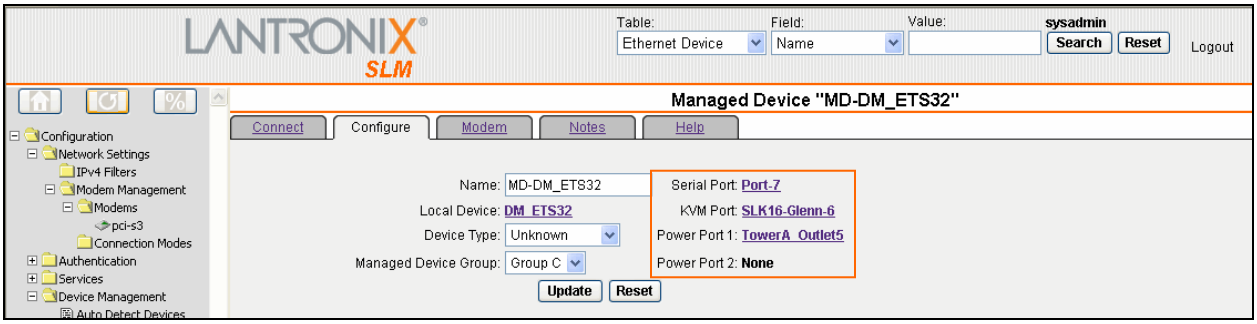
5. On the menu, click the virtual managed device. The **Connect** tab displays the components of the virtual managed device, each with the button(s) for connecting directly to each component.

Figure 9-20. Virtual Managed Device after Fusion



6. Click the **Configure** tab to see the list of managed devices that make up the virtual managed device.

Figure 9-21. Managed Device Page – Configure Tab



Note: *You can change the name of the virtual managed device, identify the device type if a local device is a component of the virtual device, and change the Managed Device Group to which the virtual managed device belongs.*

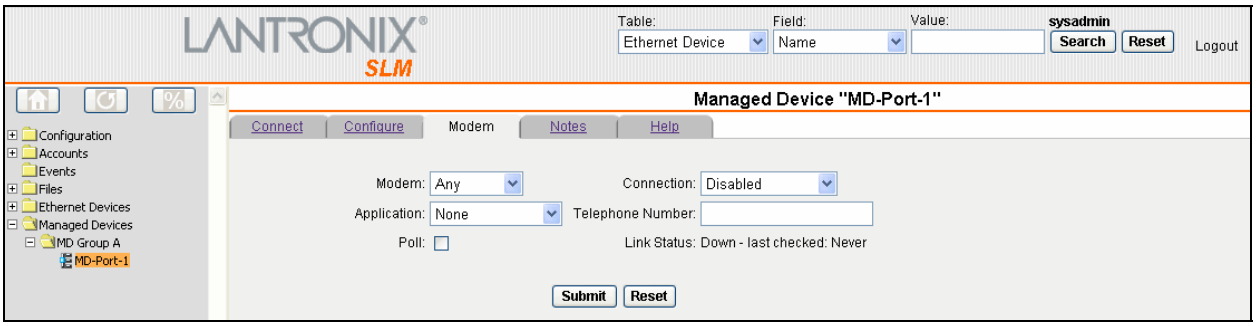
Configuring a Modem Connection to a Managed Device

It is useful to enable the SLM to connect over the telephone should a network connection fail. This is possible if, for example, the SLM has an internal or a physically connected modem, and a managed device such as a UNIX server on the network is connected to a modem .You can connect to an SLC through a modem if you configure the SLC as a managed device. Then the SLM can connect to the SLC's attached devices through the modem.

To configure a managed device to use a modem:

1. On a Managed Device page, click the **Modem** tab: The following page opens:

Figure 9-22. Managed Device Page -- Modem Tab



2. Enter the following information:

Modem	From the drop-down list, select the modem.
Connection	From the drop-down list, select the type of modem connection. Disabled by default. For information about types of modem connections, see *Adding a Connection* on page 76.
Application	From the drop-down list, select the application for connecting to the managed device. The default setting is **None**. For example, if you select **Telnet**, the Telnet program launches to connect to the remote system after a PPP connection is established. If you select **None**, a set of buttons (**Secure Channel**, **SSH, Telnet**, **HTTP**, and **HTTPS**) displays, enabling you to select a connection method.
Telephone Number	Telephone number of the modem on the managed device
Poll	Select the check box to enable polling of the modem connection Disabled by default. (See *Configuring Polling Settings* on page 161.)
Link Status (display only)	Indicates whether the modem connection is active.

3. Click the **Submit** button. A message in the message area indicates that the managed device has been updated.

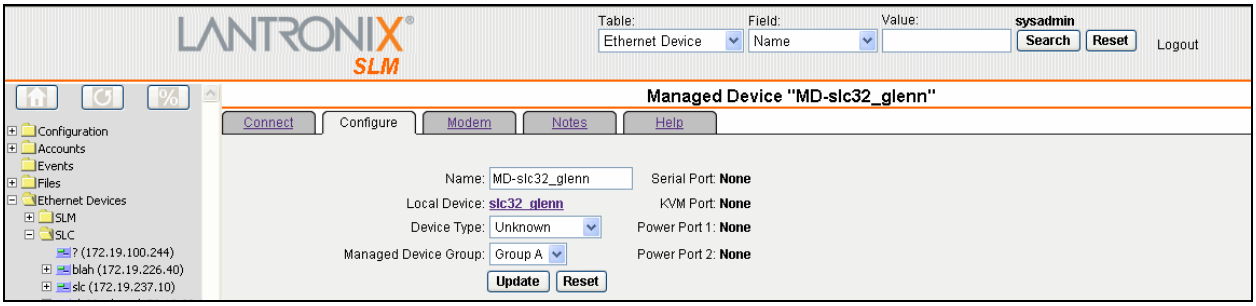
Configuring a Managed Device

The administrator and permitted users can configure a managed device.

To configure a managed device:

1. On the menu, click the name of the managed device, and then click the **Configure** tab. The following page opens:

Figure 9-23. Managed Device Page – Configure Tab



2. Edit the following information as desired:

Name	A name to identify the managed device.
Local Device	Name of an optional local Ethernet device that is being managed.

Device Type	From the drop-down list, select the type of device. Examples are **Cisco IOS**, **EMS, Firewall**, **Solaris Server**, and **Switch**. **Unknown** is the default. ***Note:*** *If you set the type to Windows, the* ***Remote Desktop*** *button displays on the* ***Connect*** *Tab.*
Managed Device Group	To change the group to which the managed device belongs, select the group from the drop-down list.

3. View the connection information in the column on the right:

Serial Port	Indicates whether the managed device is connected to a serial port on an SLC or SCS. The default is **None**.
KVM Port	Indicates whether the keyboard, video, mouse connector of the managed device is connected to a port on an SLK. The default is **None**.
Power Point 1 and 2	Indicates whether the managed device is connected to a power port on an SLP. The default is **None**.

4. To save any changes, click the **Update** button.

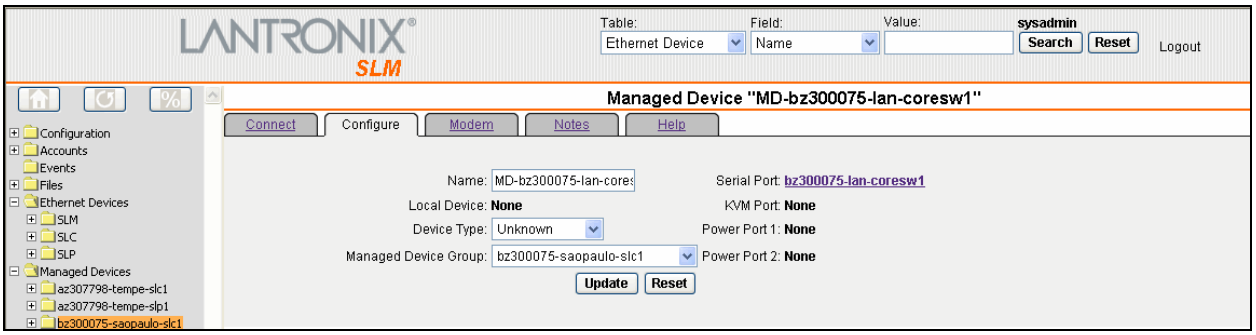
Updating or Deleting a Managed Device

The administrator and permitted users can update or delete a managed device.

To update a managed device:

1. On the menu, click the managed device. The following page opens:

Figure 9-24. Managed Device – Configure Tab



2. Add or change the entries and click the **Update** button.

To delete a managed device:

1. On the menu, click **Managed Devices**. The **Managed Devices – List** tab displays.
2. Check the managed devices that you wish to delete, and click **Delete** button at the bottom of the page.

Managed Device Commands

Administrators, Ethernet Account Users and Menu Only Users

set manageddevice config

Syntax

```
set manageddevice config <Device Name> <one or more parameters>
```

Parameters

```
name <New Name>
powerport <1|2> state <on|off|cyclepower>]
[dialout <Dial Account Name|enable|disable>
modem <Modem Name>
```

To set modem parameters, you must specify the dial-out option.

```
phonenumber <phone number>]
application <ssh|telnet|http|none>]
```

Examples

```
set ma config port-1 name waimea-port-1
```

Specifies a managed device name (port-1) and renames it to waimea-port-1.

```
set ma config slp-sunset-port1 state off
```

Specifies a managed device name (slp-sunset-port1) and turns the power off.

Description

Finds a managed device using device name and modifies device parameters.

Note: *Type* `show manageddevice all` *to display index.*

set manageddevice index

Syntax

```
set manageddevice index <number> <one or more parameters>
```

Parameters

```
name <New Name>
powerport <1|2> state <on|off|cyclepower> (SLP only)
dialout <Dial Account Name|enable|disable>
modem <Modem Name>
```

To set modem parameters, you must specify the dial-out option.

```
phonenumber <phone number>
application <ssh|telnet|http|none>
```

Examples

```
set ma config port-1 name waimea-port-1
set ma config slp-sunset-port1 powerport 1 state off
set ma index 1 dialout myaccount modem pci-s4 phone 3334444
```

If you set `dialout myaccount first` and then decide to set `modem` and `phonenumber` later, you still must specify `dialout myaccount` or `dialout enable`.

```
set ma index 1 dialout myaccount
```

```
set ma index 1 dialout enable modem pci-s4 phone 3334444
```

Description

Finds managed device by index and modifies device parameters.

set manageddevice config <Device Name> disconnect modem

Syntax

```
set manageddevice config <Device Name> disconnect modem
```

Description

Finds managed device by name and disconnects modem.

set manageddevice index <number> disconnect modem

Note: *Type `show manageddevice all` to display index.*

Syntax

```
set manageddevice index <number> disconnect modem
```

Example

```
set ma index 2 disconnect modem
```

Description

Finds managed device by index number and disconnects modem.

show device

Syntax

Note: *Entries are not case sensitive.*

```
show device <device name>
```

Description

Searches for and displays Ethernet or managed devices by device name. For example, if you specify `name slc`, the SLM searches for all Ethernet and managed devices whose name starts with `slc`.

show device all

Syntax

```
show device all
```

```
show device
```

Description

Displays all Ethernet and managed devices.

show manageddevice all

Syntax

```
show manageddevice all
```

```
show manageddevice
```

Description

Displays information about all managed devices.

show manageddevice config

Note: *Type* `show manageddevice all` *to display index.*

Syntax

```
show manageddevice config <Device Name>
```

Description

Displays the configuration of a managed device.

show manageddevice index

Syntax

```
show manageddevice index <number>
```

Description

Displays managed devices by index.

show manageddevice search

Syntax

```
show manageddevice search <one or more parameters>
```

Parameters

Note: *Search entries are not case sensitive.*

```
[name <Port Name>]
```

Examples

```
show manageddevice search name waimea-port
```

Description

Displays all ports that match the criteria entered.

Managed Device Users

set manageddevice config

Syntax

```
set manageddevice config <Device Name> <one or more parameters>
```

Parameters

```
[name <New Name>]
```

```
[state <on|off|cyclepower>]
```
(available for SLP only)
Powers managed device on or off.

Examples

```
set ma config port-1 name waimea-port-1
```
Specifies a managed device name (port-1) and renames it to waimea-port-1.

```
set ma config slp-sunset-port1 state off
```

Specifies a managed device name (slp-sunset-port1) and turns the power off.

Description

Finds a managed device-by-device name and modifies device parameters.

set manageddevice index

Note: *Type* `show manageddevice` *all to display index.*

Syntax

```
set manageddevice index <number> <one or more parameters>
```

Parameters

```
name <New Name>
powerport <1|2> state <on|off|cyclepower>] (SLP only)
```

Example

```
set ma port slp-sunset po 2 state on
```

Description

Finds managed device by index and modifies device parameters.

set manageddevice config <Device Name> disconnect modem

Syntax

```
set manageddevice config <Device Name> disconnect modem
```

Description

Finds managed device by name and disconnects modem.

set manageddevice index <number> disconnect modem

Note: *Type* `show manageddevice all` *to display index.*

Syntax

```
set manageddevice index <number> disconnect modem
```

Example

```
set ma index 2 disconnect modem
```

Description

Finds a managed device by index number and disconnects modem.

10: Operation and Maintenance

Depending on permissions, the typical user employs SLM to:

- Search for SLCs and other Ethernet devices, ports, and managed devices.
- Connect by browser, SSH, or secure channel to SecureLinx devices and to the managed devices connected to their ports.
- Access notes and logs about the Ethernet devices and their ports.

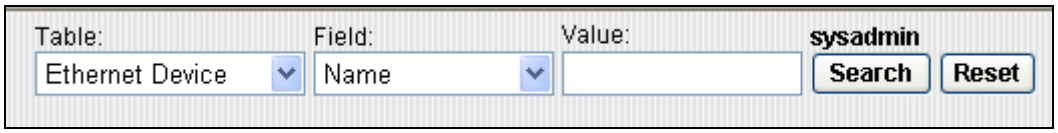
The administrator performs the following maintenance activities:

- Update SLM firmware and configurations
- Configure and manage log files
- Configure an SNMP agent
- View events
- Update SLC firmware

Searching for Ethernet Devices, Ports, Managed Devices, and Users

All pages in the web interface have three search fields at the top. Administrators and Ethernet Device Account groups can search by Ethernet device, port, and managed devices. Administrators with account rights can also search by user. Managed Device Account Groups can only search by managed device.

Figure 10-1. Search Fields



To view or make changes to any item returned in a search, click the **Edit** icon in the leftmost column. (If the search returns the item, you have rights to edit it.)

To clear the search fields, click the **Reset** button. To re-sort the list (e.g., alphabetically by name), click the header of the column you want to sort by.

All searches are case insensitive.

Search for an Ethernet Device

There are several criteria to use to search for an Ethernet device.

To search for Ethernet devices on the network:

1. From the **Table** drop-down list at the top of any page, select **Ethernet Device**.
2. From the **Field** drop-down list, select one of the following search fields and enter the corresponding **Value**. If you omit the value, the search returns all devices.

Note: Searches are not case sensitive.

Device Fields	**Name:** The name of the device for which you are searching. You need type only as many characters as will identify the device. For example, **s** returns all devices with names starting with **s**. **IP Address:** The IP address of the device for which you are searching. You need enter only as many octets as will identify the device or group of devices. **Location:** The location of the device (or devices), for example, a room or building. You need type only as many characters as will identify the location. Thus, **Irv** returns all devices with locations starting with **Irv**, for example, Irvine. Case insensitive. **Model:** Model name of the device(s) (e.g., SLC16, SLM 2.0). **Firmware:** Version of the device's firmware (e.g., 4.0).

3. Click the **Search** button. The Search Results - Devices page opens, listing all devices that meet the search criteria that you have permission to see.

Figure 10-2. Example of a Search by IP Address

Search Results - Devices

Name	IP Address	Ethernet Address	Device Type	Location	Model	FW Ver	Last FW Update	Login	Channel Key	Poll	Reach Fail Count	SSH Port
172.18.18.40	172.18.18.40	00:20:4A:80:8C:04	Spider		SLS			sysadmin	No	Yes	0	22
172.18.18.42	172.18.18.42	00:80:A3:8C:00:37	Spider		SLS			sysadmin	No	Yes	0	22
Chicago	172.18.18.50	00:80:A3:89:06:23	SLC	Irvine	SLC16	4.4		sysadmin	No	Yes	0	22
conserver	172.18.0.86	08:00:20:FE:59:8C	Non Lantronix	"System administrators office"					No	Yes	0	22
KVM	172.18.0.217	00:80:A3:88:27:91	SLK	Server-room	SLK				No	Yes	0	22
KVM	172.18.0.216	00:80:A3:88:27:4A	SLK	Server-room	SLK				No	Yes	0	22
MPS_1F05F9	172.18.0.104	00:80:A3:1F:05:F9	Non Lantronix	MPS100					No	Yes	0	22
SCS3205.support.int.lantronix.com	172.18.21.115	00:30:31:00:52:18	Non Lantronix	Lantronix Milford					No	Yes	5134	22
SCS4805	172.18.18.151	00:00:00:00:00:00	SCS05/20		SCS4805				No	Yes	0	22
SecureLinxSLP_8b0035	172.18.18.51	00:80:A3:8B:00:35	SLP	No Location	SLP	5.3a	(FW update success - 04/03 19:23)	sysadmin	No	Yes	0	22
SecureLinxSLP_8b0133	172.18.0.108	00:80:A3:8B:01:33	SLP	No Location	SLP	5.3i	(FW update success - 04/03 20:27)	sysadmin	No	Yes	0	22
SLK8-JV	172.18.18.100	00:80:A3:88:01:D1	SLK	test	SLK			root	No	Yes	0	22
tsacs16dp	172.18.1.102	00:60:2E:00:4E:CF	Non Lantronix	AlterPath_ACS					No	Yes	0	22
TSCatalystSW	172.18.0.109	00:01:96:90:09:01	Non Lantronix						No	Yes	5135	22
TSCatalystSW.support.int.lantronix.com	172.18.21.66	00:01:96:90:09:00	Non Lantronix	Michael Lyon's Cubicle					No	Yes	0	22
TS_HPUX	172.18.0.50	08:00:09:F2:DA:74	Non Lantronix						No	Yes	0	22
tsnetrat1105	172.18.0.84	08:00:20:C1:C4:02	Non Lantronix	System administrators office					No	Yes	0	22
tsslc48	172.18.21.61	00:30:31:FF:FF:42	SLC		SLC48	5.0		sysadmin	Yes	Yes	0	22
tsslc48	172.18.0.107	00:30:31:FF:FF:54	SLC		SLC32	4.3			Yes	Yes	0	22
ts-solaris10-x86	172.18.0.89	00:01:02:4F:D6:76	Non Lantronix	"System administrators office"					No	Yes	0	22
tssolaris8	172.18.0.80	08:00:20:9C:81:49	Non Lantronix	System administrators office					No	Yes	0	22
tssolaris9-x86	172.18.0.83	00:40:05:37:EF:73	Non Lantronix	System administrators office					No	Yes	5135	22
ts-sunfire280r	172.18.0.85	00:03:BA:02:A6:52	Non Lantronix	"System administrators office"					No	Yes	0	22
UDS-10/Cobox 4.X	172.18.0.101	00:20:4A:52:05:08	Other Lantronix		UDS-10/Cobox 4.X				No	Yes	0	22
WIN2KSERVER	172.18.0.12	00:D0:09:F7:5C:D5	Non Lantronix						No	Yes	0	22

25 items

The following information (if available) displays for each device retrieved by the search:

Name	Name of the device (e.g., SLC 4.0).
IP Address	IP address of the device.
Ethernet Address	Hardware or MAC address.
Location	Place at the site, such as a room or a closet, where the unit is installed.
Model	Model name of the device (e.g., SLC48).
Firmware Version	Firmware release number (e.g., 2.1).

Login	User name for accessing the device.
Channel Key	**Yes** indicates that a secure channel has been established between the SLM and the device. The **Channel Key** does not indicate whether or not there is an active secure channel communication session, but instead indicates whether or not a secure channel was established to the device in the past, enabling the SLM to connect to the device without using a password. ***Note:*** *Behind the scenes, the secure channel uses SSH keys for authentication.*
Poll	**Yes** indicates that the device may be polled.
Reach Fail Count	During polling, the SLM keeps track of the number of consecutive failures. If that count exceeds the threshold specified in **Auto Connection Fail Count** (on the Polling tab of the Ethernet Devices page), the icon for that device shows a red stripe. If that device is configured for auto-modem connect, the SLM will attempt to connect to that device over telephone lines.
SSH Port	Port assigned for SSH access, if applicable.

The Search Results - Devices page opens, listing all devices that meet the search criteria that you have permission to see.

Search for Ports

To search for a port, you can use two criteria.

To search for a port:

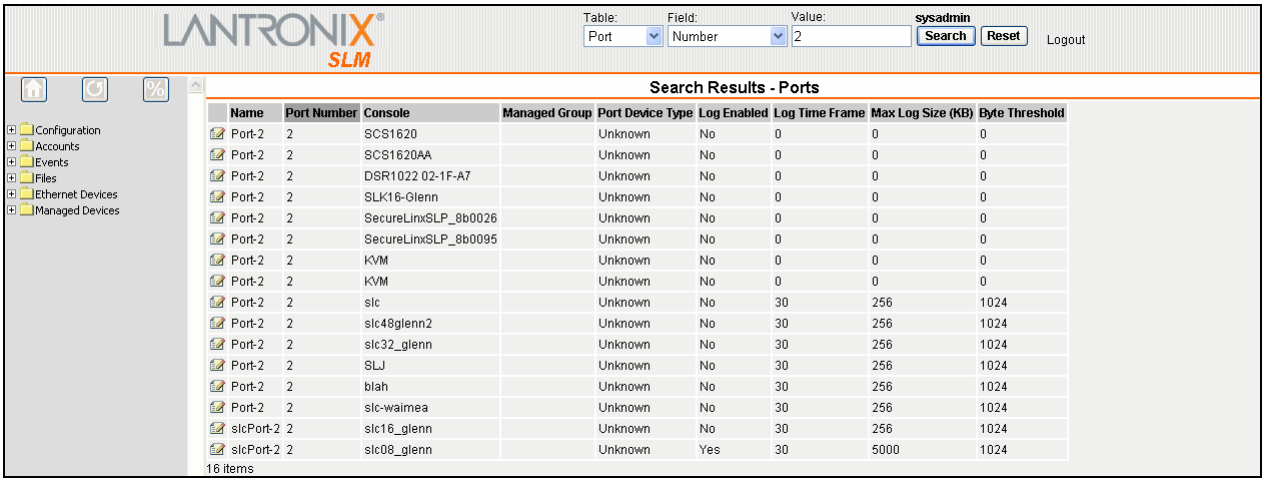
1. From the **Table** drop-down list at the top of any page, select **Port**.
2. From the **Field** drop-down list, select one of the following and enter the corresponding **Value**. If you omit the value, the search returns all ports.

Note: *All searches are case insensitive.*

Port Fields	**Name:** The name of the port for which you are searching. You need type only as many characters as will identify the port. For example, **s** returns all devices with names starting with **s**. **Number:** Number of the port for which you are searching.

3. Click the **Search** button. The Search Results - Ports page opens, listing all ports that meet the search criteria that you have permission to see.

Figure 10-3. Example of a Search by Port


LANTRONIX SLM
Table: Port
Field: Number
Value: 2
sysadmin
Search
Reset
Logout
Configuration
Accounts
Events
Files
Ethernet Devices
Managed Devices
Search Results - Ports
Name | Port Number | Console | Managed Group | Port Device Type | Log Enabled | Log Time Frame | Max Log Size (KB) | Byte Threshold
Port-2 | 2 | SCS1620 | | Unknown | No | 0 | 0 | 0
Port-2 | 2 | SCS1620AA | | Unknown | No | 0 | 0 | 0
Port-2 | 2 | DSR1022 02-1F-A7 | | Unknown | No | 0 | 0 | 0
Port-2 | 2 | SLK16-Glenn | | Unknown | No | 0 | 0 | 0
Port-2 | 2 | SecureLinxSLP_8b0026 | | Unknown | No | 0 | 0 | 0
Port-2 | 2 | SecureLinxSLP_8b0095 | | Unknown | No | 0 | 0 | 0
Port-2 | 2 | KVM | | Unknown | No | 0 | 0 | 0
Port-2 | 2 | KVM | | Unknown | No | 0 | 0 | 0
Port-2 | 2 | slc | | Unknown | No | 30 | 256 | 1024
Port-2 | 2 | slc48glenn2 | | Unknown | No | 30 | 256 | 1024
Port-2 | 2 | slc32_glenn | | Unknown | No | 30 | 256 | 1024
Port-2 | 2 | SLJ | | Unknown | No | 30 | 256 | 1024
Port-2 | 2 | blah | | Unknown | No | 30 | 256 | 1024
Port-2 | 2 | slc-waimea | | Unknown | No | 30 | 256 | 1024
slcPort-2 | 2 | slc16_glenn | | Unknown | No | 30 | 256 | 1024
slcPort-2 | 2 | slc08_glenn | | Unknown | Yes | 30 | 5000 | 1024
16 items

The following information (if available) displays for each port retrieved by the search that you have permission to see:

Name	Name of the device connected to the port.
Port Number	Number of the port.
Console	Name of the Ethernet device.
Managed Group	Name of the group of managed devices to which this device belongs.
Port Device Type	Type of managed device (e.g., Linux Server).
Log Time Frame	**For SLC v3.1 and later v3.x (but not v4.0):** The maximum time frame in hours before a new log file is created. The default setting is **1** hour. **For SLC v4.0 and later:** The maximum time frame *in seconds* before the SLC sends data to the SLM. The default setting is **30** seconds.
Max Log Size (KB)	Maximum size of each log file in kilobytes. Once it is reached, a new log file is created.
Byte Threshold	The number of bytes of data the port receives before the Ethernet device captures log data and sends a notification regarding this port.

4. The Search Results - Ports page opens, listing all ports that meet the search criteria that you have permission to see.

Search for Managed Devices

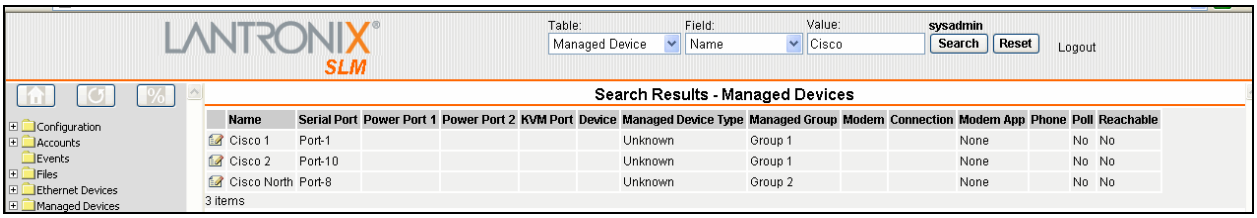
To search for a managed device, Administrators, Ethernet Device Account group members, and Managed Device Account Group members can search by name.

To search for managed devices on the network:

1. From the **Table** drop-down list at the top of any page, select **Managed Device**.
2. From the **Field** drop-down list, select **Name** and the corresponding **Value**. If you omit the value, the search returns all managed devices.

3. Click the **Search** button. The Search Results - Devices page opens, listing all managed devices that meet the search criteria that you have permission to see.

Figure 10-4. Example of a Search by Managed Device



The following information (if available) displays for each managed device retrieved by the search that you have permission to see:

Name	Name of the managed device.
Serial Port	Number or name of the Ethernet device's serial port (e.g., a number between 1 and 48 for the SLC 48) that is connected to the managed device's console port.
Power Port 1	Number or name of an SLP's power port that is connected to the managed device's power connector.
Power Port 2	Number or name of an SLP's second power port that is connected to the managed device's power connector.
KVM Port	Number or name of an SLK (KVM) port that is connected to the managed device's KVM port.
Device	Name of the Ethernet device.
Managed Device Type	Type of managed device (e.g., Solaris Server or Linux Server).
Managed Group	Name of the Managed Device Group to which the managed device belongs.
Modem	Name of the modem to be used when connecting to the managed device.
Connection	Type of connection to make when using the modem.
Modem App	Application to invoke for the connection (e.g., Secure Channel, SSH, Telnet).
Phone	Telephone number of the modem on the managed device.
Poll	Indicates whether to check the managed device for modem connectivity during modem polling testing.
Reachable	Indicates whether a connection to the modem on this managed device was successful the last time it was tested.

Search for Users

To search for users, administrators with account rights can search using two criteria.

To search for users on the network:

1. From the **Table** drop-down list at the top of any page, select **User**.
2. From the **Field** drop-down list, select one of the following search fields and enter the corresponding **Value**. If you omit the value, the search returns all devices.

Note: Searches are not case sensitive.

User Fields	**Name:** The name of the user for whom you are searching. You need type only as many characters as will identify the user. For example, **s** returns all users with names starting with **s**. **E-Mail:** E-mail address of the user for whom you are searching.

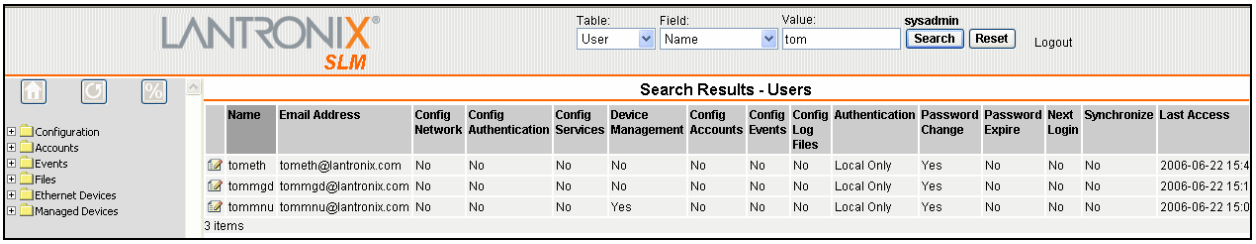
3. Click the **Search** button. The Search Results - Users page opens, listing all users who meet the search criteria.

The following information (if available) displays for each user retrieved by the search.

Name	The user name for logging in to the SLM.
Email Address	User's email address; may be used for event notification.
Config Network	**Yes** indicates the user can open the Network Settings page and configure network settings.
Config Authentication	**Yes** indicates the user can select and prioritize authentication methods and related settings.
Config Services	**Yes** indicates the user can configure services such as date and time and SNMP Agent & syslog and update SLCs to which the user has access.
Device Management	**Yes** indicates the user can configure settings for auto-detecting devices and ports and for managing alternate SLMs.
Config Accounts	**Yes** indicates the user can add, update, and delete all accounts and grant account permissions.
Config Events	**Yes** indicates the user can set alarms and triggers.
Config Log Files	**Yes** indicates the user can view, copy, and delete various log files.
Authentication	Indicates whether authentication for this user is **Local Only**, **Remote Only**, **Local & Remote**, or **Disabled**.
Password Change	**Yes** indicates that the user can use the current password indefinitely. Selected by default.
Password Expire	**No** allows the user to keep a password indefinitely.
Next Login	**Yes** requires the user to change the password the next time the user logs in. (You may change this setting at any time.)

Synchronize	**Yes** indicates that if the user's password has changed since the last synchronization, the SLM will update that new password on all SLMs, SLCs, SCSxx05/20s, and SLPs.
Last Access	Date and time the user last logged into the SLM, or the date and time of account creation if the user has never logged in.

Figure 10-5. Example of a Search by User



Using Wildcards

You can use SQL wildcards when conducting a search:

- Use the percent sign (%) to match zero or more instances of any character.
- Use the underscore (_) to match any one character.

Note: *The SLM search automatically appends a percent sign to the end of all search strings, so you do not need to put one there. All searches are case insensitive.*

A search for _abc will find:	A search for %abc will find:	A search for s___2 (three underscores) will find
Aabc BABCdef AabCghi bAbC	aaaaaaaabCccccccc ABCccccccccccccc jjjjjjjjjjjabc	SLM32_device Sxx32 s2232_system
but not	*but not*	*but not*
aaabcdc	Aaaaaaaabbcccccc Bccccccccccccccc Jjjjjjjjjjjab	SLM332_device sAB16 Dev_2232

Search Commands

show account search email

Syntax

show account search email <email address>

Example

```
show account search email sys
```

Displays all accounts whose email address starts with "sys."

Description

Displays accounts that match the email address entered.

show account search name

Syntax

```
show account search name <user name>
```

Examples

```
show account search name sys
```

Displays all accounts whose name starts with "sys."

Description

Displays accounts that match the name entered.

show ethernetdevice search device

Syntax

```
show ethernetdevice search device <one or more parameters>
```

Parameters

Note: *Search entries are not case sensitive.*

```
[name <Device Name>]
[ipaddr <IP Address>]
[location <location>] [firmware <version number>]
```

Example

```
show ethernetdevice search device name slc firmware 4
```

Description

Displays all devices that match the criteria entered. For example, if you specify `name slc`, the SLM searches for all devices whose name starts with `slc`.

show ethernetdevice search port

Syntax

```
show ethernetdevice search port <one or more parameters>
```

Parameters

Note: *Search entries are not case sensitive.*

```
[name <Port Name>]
[portnumber <Port Number>]
```

Example

```
show ethernetdevice search port name waimea-port
show ethernetdevice search port name waimea portnumber 2
```

Description

Displays all ports that match the criteria entered.

show manageddevice search

Syntax

```
show manageddevice search <one or more parameters>
```

Parameters

Note: *Search entries are not case sensitive.*

```
[name <Port Name>]
```

Example

```
show manageddevice search name waimea-port
```

Description

Displays all ports that match the criteria entered.

Connecting to Ethernet and Managed Devices

Connections Overview

From the SLM, you can connect to SecureLinx management and other Ethernet devices just as you would if you logged into the device directly. You can also connect to Managed Devices.

Permissions set on the SLM for Ethernet devices and managed devices, in addition to granting access to device information in the SLM database, determine whether an account group can manage or just listen to the device.

Connection methods offered on a Managed Device depend on what is being managed, as well as the device types doing the management. For instance, if a Linux Server is being managed, then a **VPN** connection button displays. If a Windows box is being managed, then **Remote Desktop** is offered. Other connection methods are offered according to the device type specified in the table above.

Note: *Some buttons on Device and Port pages may be inactive, depending on the type of device. On the Managed Device page, only active buttons display.*

Ethernet Devices – Connection Methods

The table below shows the methods available for connecting to an Ethernet device.

Methods of Connecting to Ethernet Devices

Ethernet Device	Browse HTTP	Browse HTTPS	Secure Channel	Web Channel	SSH	Telnet
SLM	X	X	X		X	X
SLC		X	X	X	X	X
SLK	X	X				X
SLP	X	X			X	X
SLB		X	X	X	X	X
Spider	X	X	X	X	X	X
SCS05/20		X			X	X
SCSxx00	X	X			X	X
WiBox	X					X
UDS	X					X
Other Lantronix	X	X			X	X
Other Devices (Non-Lantronix)	X	X			X	X

Managed Devices – Connection Methods

The following table shows the methods available for connecting to a managed device.

Methods of Connecting to Managed Devices

Managed device connected to:	Connection methods
Non-Lantronix, SCS05/20, SCSxx00, Other Lantronix	By means of SSH when connected by serial; when a local Ethernet device is being managed, then HTTP, HTTPS, SSH, Secure Channel, Telnet, and Remote Desktop may be offered, depending on the type of Ethernet device.
SLK	HTTP or HTTPS
SLC and SLM	Secure Channel; also Web Channel for SLC

Note: *Depending on the device, some of the buttons may be inactive.*

Browsing to an Ethernet or Managed Device's Web Page

Users can browse directly to the home page of a SecureLinx or other discovered Ethernet device.

Note: *If the **Login** and **Password** fields in the device record have been completed, the SLM uses them for an automatic login when you browse to secure devices. However, if you use Microsoft Internet Explorer on the client machine, you must change the registry to use this feature. Netscape and Firefox do not have this problem. You can change the Windows registry with the file included in the CD, **iefix.reg**. You must run this file on the client machine that runs IE. Further, some non-Lantronix devices (notably the Avocet DSR1022) require IE 7 to support the browsing feature (from SLM to other device).*

Warning: ***If you use this method of automatic login, the password stays as part of your browser history. Make sure to clear the web history if you want to eliminate the possibility of another person learning your password by looking through your browser history. In general, only use this method of automatic login within a facility where only trusted personnel have access.***

To access the Ethernet device's web page interface:

1. On the Device page, click the **Browse http** or **Browse https** button.
2. If required, enter the user name and password for accessing the device. The device's home page opens.
3. Configure or manage the device as directed by the device's User Guide or online Help.

Making a Secure Channel Connection to an SLC, SLM, or SLB

You can use a Lantronix secure channel connection from the web interface to the command line interface of another SLM or an SLC and its ports and managed devices.

Secure channel is actually a special form of SSH connection. If you use the secure channel, you need only supply the password when logging into the SLM. If you use SSH, you have to supply the password every time.

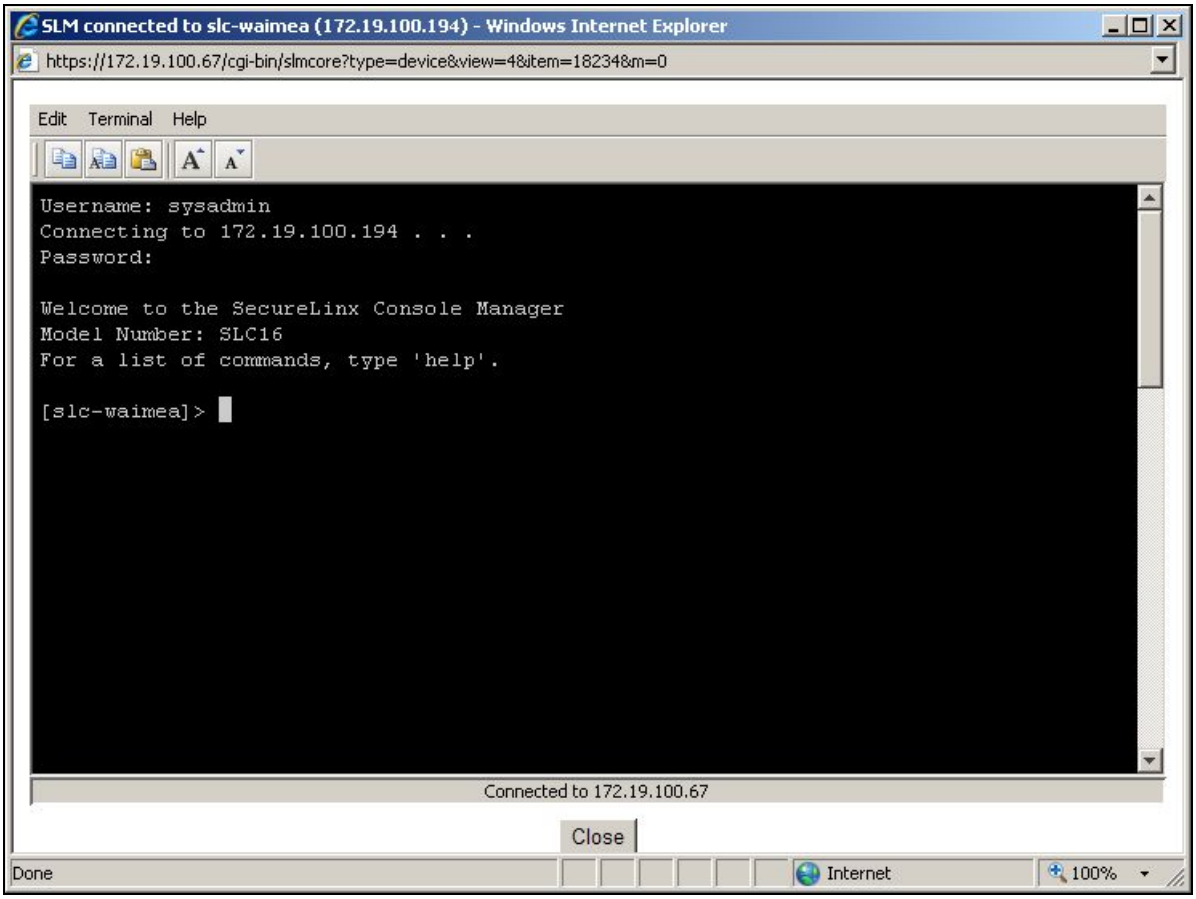
Before connecting to an SLC or to another SLM through the secure channel, the administrator must first establish the secure channel connection to the Ethernet device (SLC or SLM only). The administrator attempts to connect to the Ethernet device through the SLM secure channel connection and supplies the **sysadmin** password for the SLC. After this, any authenticated user who has permission to connect to the Ethernet device can connect to it through the SLM secure channel without further authentication.

Configure or manage the device as directed by the product's User Guide or online Help.

To make a secure channel connection to an SLC or SLM:

1. To log in to the SLC, SLB, or SLM, click the **Secure Channel** button on its Ethernet device page. A Java applet runs, and then the "Connected to SLM" message displays.

Figure 10-6. Secure Channel Connection to an SLC



2. If prompted to enter a key, type **Yes** to continue.
3. If prompted, enter your current **sysadmin** password for the SLC.
4. Configure or manage the device as directed by the product's User Guide or online Help.

Following is a list of error codes that may display:

Secure Channel Error Codes		
Major Code	**Minor Code**	**Description**
1	40	Could not connect to SLC
1	41	Network connection to SLC broken during login
1	50	Error opening secure channel key
1	51	Error reading secure channel key
3	62	Error removing old secure channel key from SLC
3	64	Error importing secure channel key to SLC
4	68	Error importing secure channel key to SLC
4	80	Error assigning user permissions
6	81	Timeout connecting to device port
6	101	Error connecting to device port (the port may already be in use)
6	102	Error listening to device port. (the port may not be connected)
8	200	Error getting key data from SLC
8	202	Error establishing secure channel session to SLC

Secure Channel Error Codes		
8	203	Error establishing connection to SLC
10	204	Error updating secure channel status
11	205	Error setting user permissions (for a connection to a device port)
X	207	Error exiting device port access
X	301	Error exiting listen mode
X	600	Error setting user permissions (for a connection to the CLI)
X	800	Error clearing command history on SLC

Note: *Error codes display in the format: <Major Code>,<Minor Code>. An **X** indicates a variable major code.*

Making an SSH Connection to an Ethernet or Managed Device

Users can use SSH from the web page of a Java-enabled web browser to connect to the command line interface of any SecureLinx or other discovered Ethernet device.

SSH is a connection protocol that requires all data sent to be encrypted. SSH accomplishes this by using public and private keys generated by the client and the server. Both sides have a pair of keys. The private key encrypts the data being sent; for the receiver to decrypt the received encrypted data, it must have the sender's public key.

The received host key is saved in a file called **known_hosts** in the SSH directory of users. Upon reconnection to the same host, the receiver compares the newly received host key to the previously received key that was stored in the **known_host** file.

If the newly received host key matches the key in the **known_host** file, then the authentication process (login and password) continues.

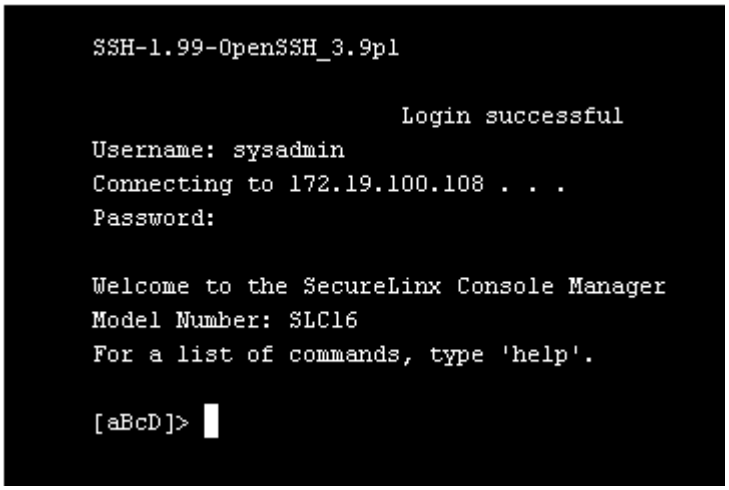
If the newly received host key does not match the key in the **known_host** file, then the user receives a warning that they do not match and is asked whether to replace the old host key information with the new key. (There could be someone trying to impersonate the known host.)

If the newly received host key does not exist in the **known_host** file, the device warns the user that the host does not exist (first-time connection) and asks the user if it should add the new key to the **known_host** file.

To make an SSH connection to the device CLI:

1. To log in to a SecureLinx management device using SSH, click the **SSH** icon. A Java applet runs.
2. In response to the prompts, enter the user name and password for the device.

Figure 10-7. SSH Login to SLC



3. Configure or manage the device as directed by the device's User Guide or online Help.

Making a Web Channel Connection to an SLC

The web channel feature uses the existing secure channel key to the SLC to authenticate through the web interface. This enables an SLM user to connect to the web interface on an SLC without having to enter a username and password. The web connection to the SLC filters through the SLM. The **Web Channel** button is only active for SLCs that already have a secure channel. No other device types currently support this feature.

To make a web channel connection:

1. On an SLC that has been set up for a secure channel, click the Web Channel **button**. The SLC Web Home Page displays.

Figure 10-8. Web Channel Connection to an SLC

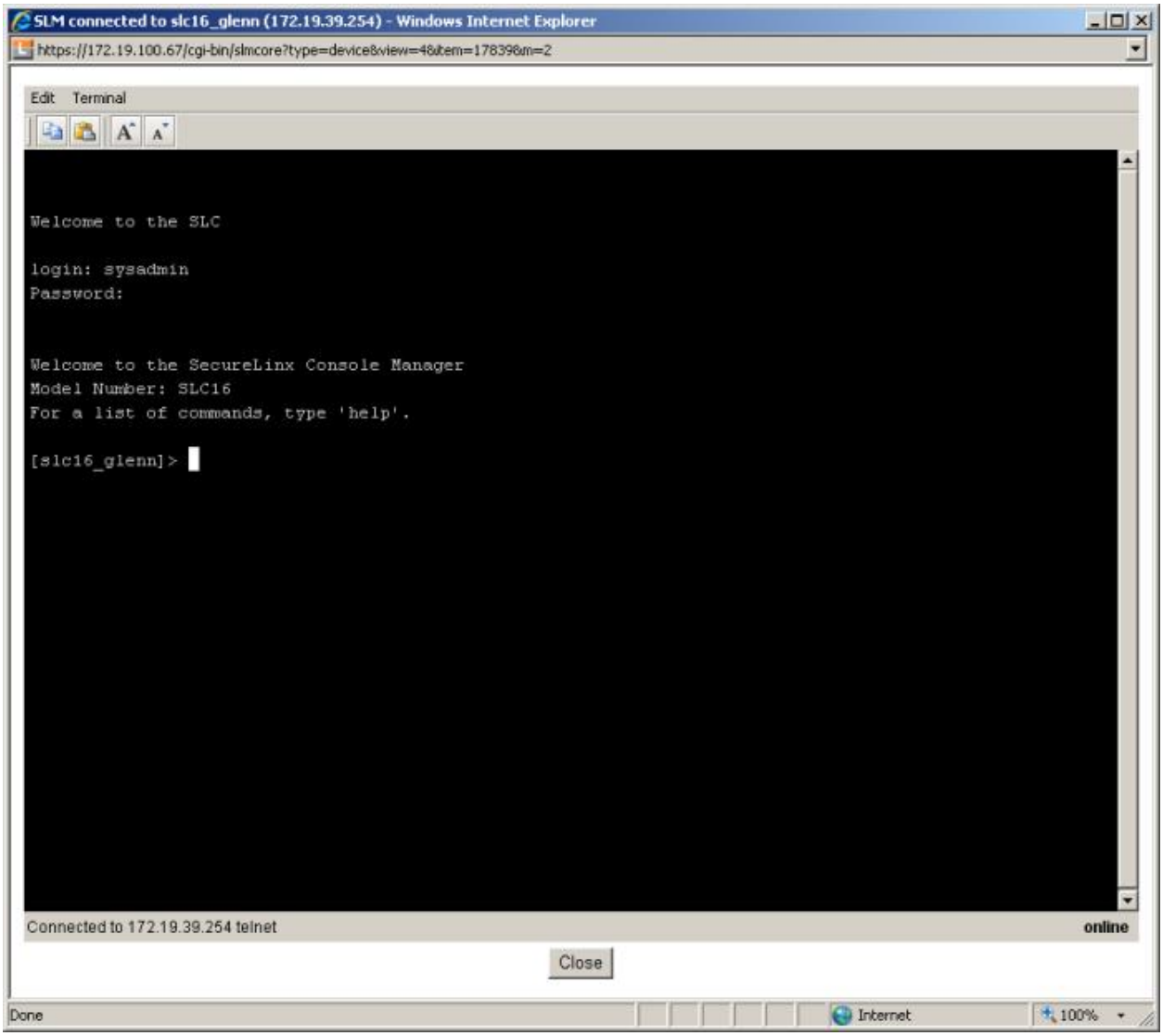
Making a Telnet Connection to an Ethernet device

You can make a Telnet connection to the command line interface of any discovered Ethernet device.

To make a Telnet connection:

1. Click the **Telnet** button. A Java applet runs, and then the Telnet command line interface displays.

Figure 10-9. Telnet Connection



2. Configure or manage the device as directed by the device's User Guide or online Help.

Connection Commands

Administrators, Ethernet Users and Menu Only Users

connect device

Syntax

```
connect device <Device Name or IP Address>
[<secure|ssh|telnet|serial|modem|modemssh|modemtelnet>] [port
<port>]
```

Specify `secure` to connect through a secure channel. Secure channel is the default method of connection for SLC, SLC ports, and SLM, and SSH is the default for other devices.

Port is the number of a physical port on the SLC.

Example

SLC48 has ports 1 to 48.

Modem connection is available for managed devices only.

With the `modemssh` option, the SLM dials out to the managed device in PPP, and then connects it via SSH.

With `modemtelnet` option, the SLM dials out to the managed device in PPP, and then connects it via Telnet.

Examples

```
connect device slc-waimea
connect device slc-waimea-port-1
connect device slc-waimea ssh
connect device slc-waimea port 4
connect device slc-waimea modemssh
```

Description

Connects to an Ethernet device, managed device, or device port.

connect index <number>

Note: *Type* `show device all` *to display the index.*

Syntax

```
connect index <number>
<secure|ssh|telnet|serial|modem|modemssh|modemtelnet>]
```

Description

Connects a device by index number.

connect ssh

Syntax

```
connect ssh <IP Address> [tcpport <TCP Port>] [<SSH flags>]
```

Parameters

`<SSH flags>` is one or more of:

```
user <Login Name>
version <1|2>
escape <Character>
```

`tcpport` is the TCP port number; the default is **22**.

Description

Connect to any machine/device using standard SSH V1 or V2 protocol.

connect telnet

Syntax

```
connect telnet <IP Address> [tcpport <TCP Port>] [user <Login Name>]
```

`tcpport` is the TCP port number; the default is **23**.

Description

Connects to a device by means of standard Telnet.

Managed Device Users

connect device

Syntax

connect device <Device Name>
`[<secure|ssh|telnet|serial|modem|modemssh|modemtelnet>] [port <port>]`

Specify `secure` to connect through a secure channel. Secure channel is the default method of connection for SLC, SLC ports, and SLM, and SSH is the default for other devices.

Port is the number of a physical port on the SLC.

Example

SLC48 has ports 1 to 48.

Modem connection is available for managed devices only.

With the `modemssh` option, the SLM dials out to the managed device in PPP, and then connects it via SSH.

With `modemtelnet` option, the SLM dials out to the managed device in PPP, and then connects it via Telnet.

Examples

```
connect device slc-waimea
connect device slc-waimea-port-1
```

```
connect device slc-waimea ssh
connect device slc-waimea port 4
connect device slc-waimea modemssh
```

Description

Connects to a managed device through a secure channel.

connect index

Note: *Type* `show manageddevice all` *to display the index.*

Syntax

```
connect index <number>
<secure|ssh|telnet|serial|modem|modemssh|modemtelnet>
```

Description

Connects to a device by index number.

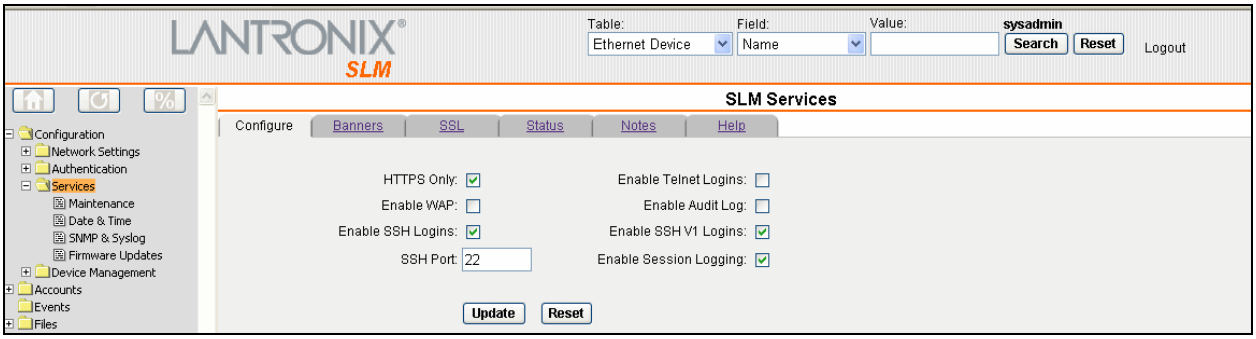
Services

The SLM Services page allows administrators to define ways to access the SLM, to configure the banner for the CLI, and to enable an audit log of the SLM.

To configure services:

1. On the menu, click **Configuration→Services**. The following page opens:

Figure 10-10. SLM Services Page



2. Enter the following information:

HTTPS Only	If selected, allows access to the SLM through HTTPS only and disallows access through HTTP. Requires a reboot to take effect. Selected by default.
Enable Telnet Logins	If selected, allows access to the SLM through Telnet. Disabled by default.
Enable WAP	If selected, allows you to access the system through a cell phone. For more information about WAP, see *11: Using SLM on a Mobile Browser*.
Enable Audit Log	If selected, enables the SLM to log all actions that have changed the configuration of the SLM. Disabled by default.
Enable SSH Logins	If selected, enables the SLM to allow users to

	access the CLI using SSH. Enabled by default.
Enable SSH v1 Logins	If selected, enables the SLM to allow users to access the CLI using SSH version 1.
SSH Port	Allows you to change the SSH TCP port to a value in the range of 1 - 65535. The default is **22**.
Enable Session Logging	If selected, enables the SLM to log data going back and forth between the user and a device or port.

3. Click the **Update** button.

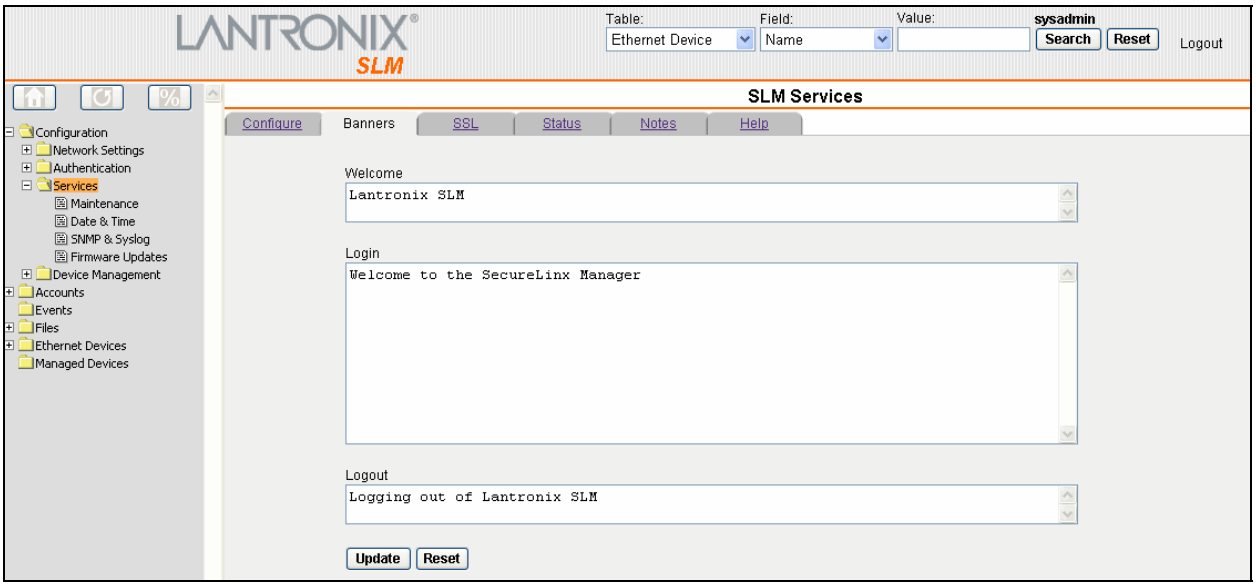
Banners

You can maintain text that is used for the CLI.

To enter banner text:

1. On the Services page, click the **Banners** tab. The following page displays:

Figure 10-11. Services Page – Banners Tab



2. Enter the following information:

Welcome	Enter the text to display at CLI connection.
Login	Enter the text to display upon successful login to the CLI.
Logout	Enter the text to display upon logout from the CLI.

3. Click the **Update** button.

Note: *Use the **Reset** button to clear the entries.*

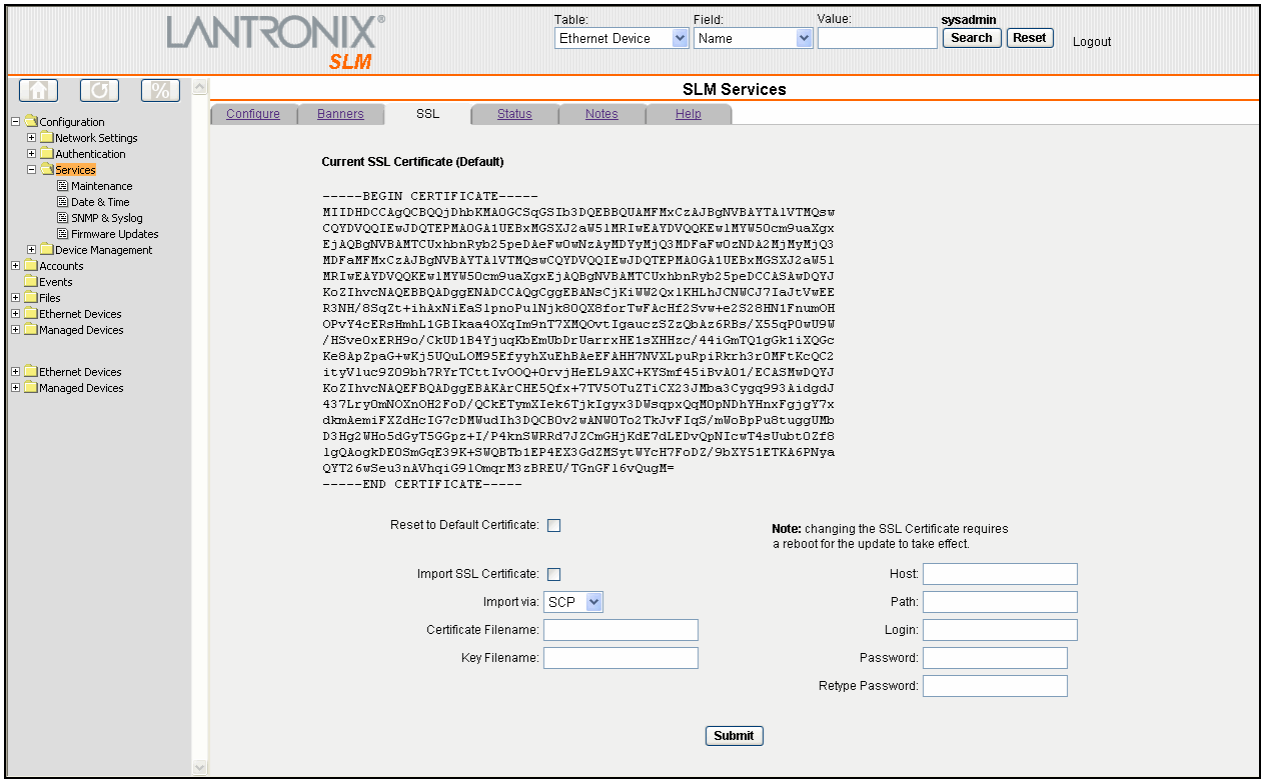
SSL

The SLM has a default Secure Socket Layer (SSL) certificate. The SSL tab enables administrators to view and update SSL certificate information. The SSL certificate, consisting of a public/private key pair used to encrypt HTTP data, is associated with the web server. You can import a site-specific SSL certificate, if desired.

To view, reset, import, or change an SSL Certificate:

1. On the Services page, click the **SSL** tab. The current certificate displays.

Figure 10-12. Services – SSLTab



2. Enter the following:

Reset to Default Certificate	To reset to the default certificate, select the checkbox to reset to the default certificate. Unselected by default.
Import SSL Certificate	To import your own SSL Certificate, select the checkbox. Unselected by default.
Import via	From the drop-down list, select the method of importing the certificate (SCP or SFTP). The default is **SCP.**
Certificate Filename	Filename of the certificate.
Key Filename	Filename of the private key for the certificate.
Host	Host name or IPaddress of the host from which to import the file.
Path	Path of the directory where the certificate will be

	stored.
Login User	User ID to use to SCP or SFTP the file.
Password & Retype Password	Password to use to SCP or SFTP the file.

3. Click the **Submit** button.

   Note: *You must reboot the SLM for the update to take effect.*

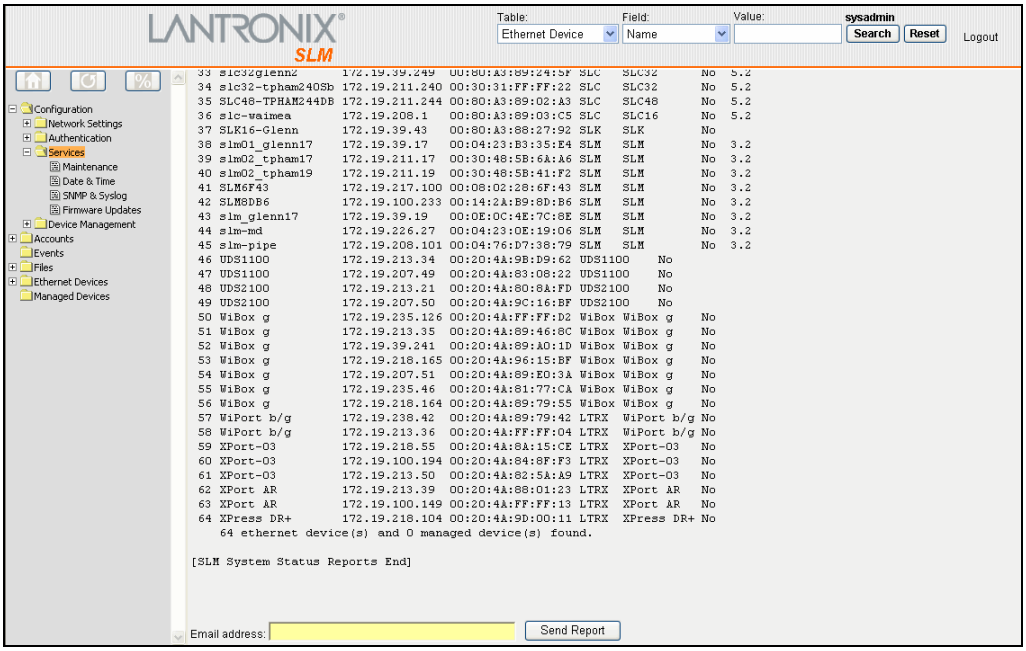
Status

Administrators can view the system status on the **Status** tab, and if they desire, email it to another person.

To view or email the system status:

1. On the Services page, click the **Status** tab. The following page displays the status information.

Figure 10-13. Services Page – Status Tab


LANTRONIX
SLM
Table:
Ethernet Device
Field:
Name
Value:
sysadmin
Search
Reset
Logout
Configuration
Network Settings
Authentication
Services
Maintenance
Date & Time
SNMP & Syslog
Firmware Updates
Device Management
Accounts
Events
Files
Ethernet Devices
Managed Devices
34 slc32-tpham240Sb 172.19.211.240 00:30:31:FF:FF:22 SLC SLC32 No 5.2
35 SLC48-TPHAM244DB 172.19.211.244 00:80:A3:89:02:A3 SLC SLC48 No 5.2
36 slc-waimea 172.19.208.1 00:80:A3:89:03:C5 SLC SLC16 No 5.2
37 SLK16-Glenn 172.19.39.43 00:80:A3:88:27:92 SLK SLK No
38 slm01_glenn17 172.19.39.17 00:04:23:B3:35:E4 SLM SLM No 3.2
39 slm02_tpham17 172.19.211.17 00:30:48:5B:6A:A6 SLM SLM No 3.2
40 slm02_tpham19 172.19.211.19 00:30:48:5B:41:F2 SLM SLM No 3.2
41 SLM6F43 172.19.217.100 00:08:02:28:6F:43 SLM SLM No 3.2
42 SLM8DB6 172.19.100.233 00:14:2A:B9:8D:B6 SLM SLM No 3.2
43 slm_glenn17 172.19.39.19 00:0E:0C:4E:7C:8E SLM SLM No 3.2
44 slm-md 172.19.226.27 00:04:23:0E:19:06 SLM SLM No 3.2
45 slm-pipe 172.19.208.101 00:04:76:D7:38:79 SLM SLM No 3.2
46 UDS1100 172.19.213.34 00:20:4A:9B:D9:62 UDS1100 No
47 UDS1100 172.19.207.49 00:20:4A:83:08:22 UDS1100 No
48 UDS2100 172.19.213.21 00:20:4A:80:8A:FD UDS2100 No
49 UDS2100 172.19.207.50 00:20:4A:9C:16:BF UDS2100 No
50 WiBox g 172.19.235.126 00:20:4A:FF:FF:D2 WiBox WiBox g No
51 WiBox g 172.19.213.35 00:20:4A:89:46:8C WiBox WiBox g No
52 WiBox g 172.19.39.241 00:20:4A:89:A0:1D WiBox WiBox g No
53 WiBox g 172.19.218.165 00:20:4A:96:15:BF WiBox WiBox g No
54 WiBox g 172.19.207.51 00:20:4A:89:E0:3A WiBox WiBox g No
55 WiBox g 172.19.235.46 00:20:4A:81:77:CA WiBox WiBox g No
56 WiBox g 172.19.218.164 00:20:4A:89:79:55 WiBox WiBox g No
57 WiPort b/g 172.19.238.42 00:20:4A:89:79:42 LTRX WiPort b/g No
58 WiPort b/g 172.19.213.36 00:20:4A:FF:FF:04 LTRX WiPort b/g No
59 XPort-03 172.19.218.55 00:20:4A:8A:15:CE LTRX XPort-03 No
60 XPort-03 172.19.100.194 00:20:4A:84:8F:F3 LTRX XPort-03 No
61 XPort-03 172.19.213.50 00:20:4A:82:5A:A9 LTRX XPort-03 No
62 XPort AR 172.19.213.39 00:20:4A:88:01:23 LTRX XPort AR No
63 XPort AR 172.19.100.149 00:20:4A:FF:FF:13 LTRX XPort AR No
64 XPress DR+ 172.19.218.104 00:20:4A:9D:00:11 LTRX XPress DR+ No
64 ethernet device(s) and 0 managed device(s) found.
[SLM System Status Reports End]
Email address:
Send Report

2. To email the status, enter the recipient's email address and click the **Send Report** button.

Services Commands

`set service auditlog`

Syntax

set service auditlog <enable|disable>

Description

Enables or disables audit logging.

set service telnet

Syntax

set service telnet <enable|disable>

Description

Enables or disables Telnet logging to the SLM.

set service ssh

Syntax

set service ssh <enable|disable> version <1|2>

Description

Enables or disables SSH logging to the SLM.

show service

Syntax

set service

Description

Displays service settings.

Maintenance

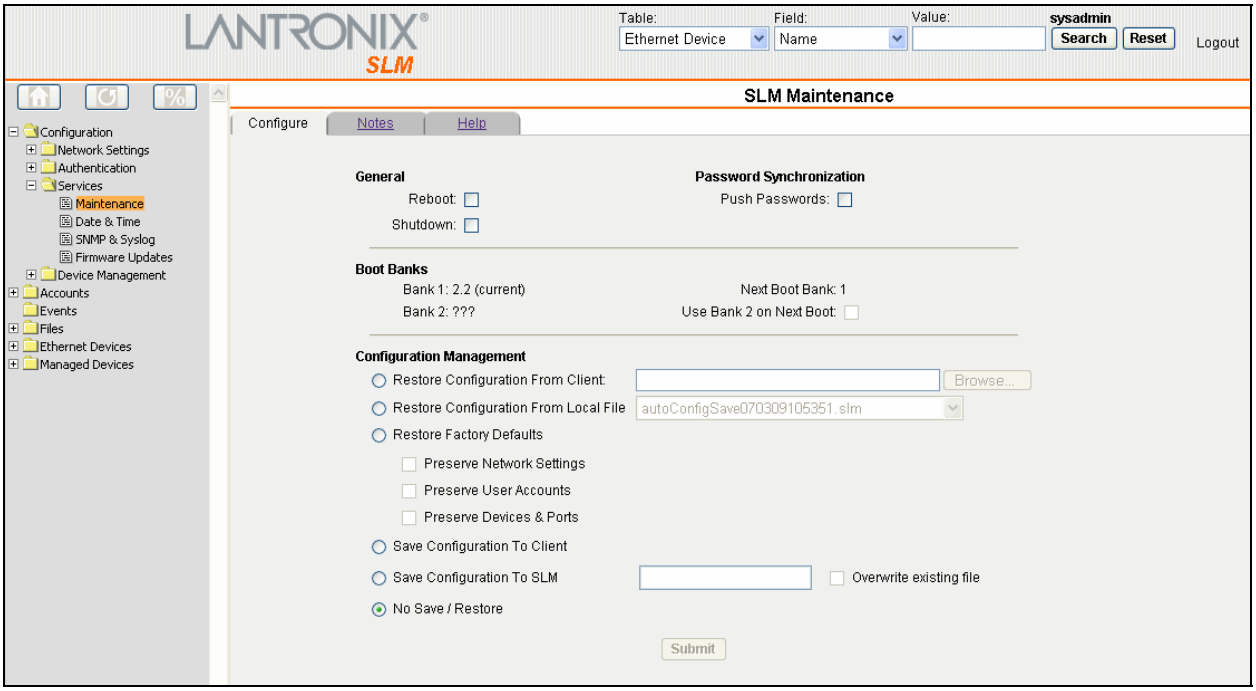
The SLM Maintenance page allows administrators to:

- Reboot or shut down the SLM.
- Save a snapshot of all database settings (configuration, configured users, and discovered devices) on the SLM or the user's client machine.
- Restore the configuration, either to a previously saved configuration or to the factory defaults.
- Update user passwords on selected SLMs/SLCs/SLBs/SLPs and SCS05/20s (password synchronization).
- View the firmware version on two boot banks, and select the bank to boot from.

To configure maintenance activities:

1. On the menu, click **Services→Maintenance**. The following page opens:

Figure 10-14. SLM Maintenance Page



General

Reboot	Select this option to terminate all connections and reboot the SLM immediately.
Shutdown	Select this option to terminate all connections, shut down the SLM immediately, and turn off the power.

Password Synchronization

Push Passwords	When the **Push Passwords** check box on the Maintenance page is selected, the SLM uses the password on all accounts with **Synchronize Password** enabled to update accounts on remote SLMs, SLCs, SLBs, SLPs and SCSxx05/20s. The accounts must have access rights to and local user accounts on the devices. For the SCSxx05/20 and SLP, you must store the username and password for each target device in the SLM, enabling password(s) to be transferred by SSH.

Boot Banks

Bank 1	Version of SLM firmware in bank 1. ***Note:*** *The word "current" displays next to the bank the SLM booted from.*
Bank 2	Version of SLM firmware in bank 2.
Next Boot Bank	Current setting for bank to boot from at next reboot.
Use Bank 2 on Next	If desired, select the bank to boot from at next

Boot	reboot.

Configuration Management

Configuration Management	From the option list, select one of the following: **Restore Configuration from Client:** Returns the SLM settings to a previously saved configuration. If you select this option, the SLM reboots after you apply the update. If you select this option, the **Browse** button becomes available. Browse to the saved configuration. **Restore Configuration from Local File:** Restores the configuration to one saved on the SLM. Select the file from the drop-down list. **Restore Factory Defaults:** Restores factory settings. If you select this option, the SLM reboots after you apply the update. To keep specific groups of settings rather than restoring defaults, select one or more of the following options: ◆ Preserve Network Settings This option preserves the settings on the Network Settings and the Services page. ◆ Preserve User Accounts ◆ Preserve Devices & Ports This option preserves Ethernet and managed devices and their groups. The three preserve options apply to any of the restore options. If you select a preserve option, then after restoration, all of the current "preserved" items are deleted, and the preserved items from before the restore are re-inserted. **Example:** You restore to a backup file but elect to preserve user accounts. The SLM is restored to the contents of the backup file, then all accounts (including any that were just restored) are deleted, and lastly, all the accounts, account groups, and notes about account groups that were present before the restore operation are added to the system. The same is true for devices and ports. If you preserve devices and ports, all associations with account groups are lost, even if both accounts and devices are preserved. ***Note:*** *If you select any of the three Restore operations, the SLM saves the current configuration in the SLM Configuration Files directory using the name autoConfigSaveYYMMDDHHMMSS.slm before performing the restore command.* **Save Configuration to Client:** Saves all settings to a file on the client system, which you can back up to a location not on the SLM. The SLM sends the file containing the state of the system to the client machine for storage. The

	default file name is **configsave.slm**, but you may save it using any name. This is the file uploaded to the SLM upon system restore. **Save Configuration to SLM:** Saves all settings to the SLM. If selected, enter the configuration file name. To overwrite the existing field with this configuration file, select the check box. Unselected by default. **No Save/Restore:** Does not save or restore a configuration.

Maintenance Commands

admin config

Syntax

```
admin config factorydefaults
```

Description

Restores the SLM configuration and device database settings to factory defaults.

admin config rebuilddatabase

Syntax

```
admin config rebuilddatabase
```

Description

Removes and rebuilds the SLM configuration and database from scratch, in case of database corruption that cannot be fixed by the factory.

admin config save file

Syntax

```
admin config save file <filename>
```

Description

Saves the SLM configuration to the SLM Configuration Files directory.

admin config showfiles

Syntax

```
admin config showfiles
```

Description

Shows saved configuration files.

admin locallog clear

Syntax

```
admin locallog clear auditlog
admin locallog clear syslog
```

```
admin locallog clear traplog device <Device Name or IP Address>
admin locallog clear traplog group <group name>
group name: SLM, SLC, SLK, SLP, SCS, LTRX, or other
```

Description

Clears all of the entries in the auditlog, syslog, or traplog.

admin quicksetup

Syntax

```
admin quicksetup
```

Description

Displays the quick setup script on the CLI; only the sysadmin account can use this command.

admin reboot

Syntax

```
admin reboot
```

Description

Terminates all connections and reboots the SLM.

admin securechannel regenkey

Syntax

```
admin securechannel regenkey
```

Description

Regenerates the secure channel key.

Note: *With this command, you lose access to established secure channels; therefore, the SLM first requests confirmation that you want to regenerate the securechannel key.*

admin shutdown

Syntax

```
admin shutdown
```

Description

Terminates all connections, shuts down the SLM, and turns off the power.

admin version

Syntax

```
admin version
```

Description

Displays current application version information.

show progress

Syntax

```
show progress
```

Description

Shows the progress of background tasks.

show sysconfig

Syntax

```
show sysconfig [email <Email Address>]
```

Description

Displays a report of configurable parameters. The output can be emailed.

show sysinfo

Syntax

```
show sysinfo
```

Description

Displays general system information.

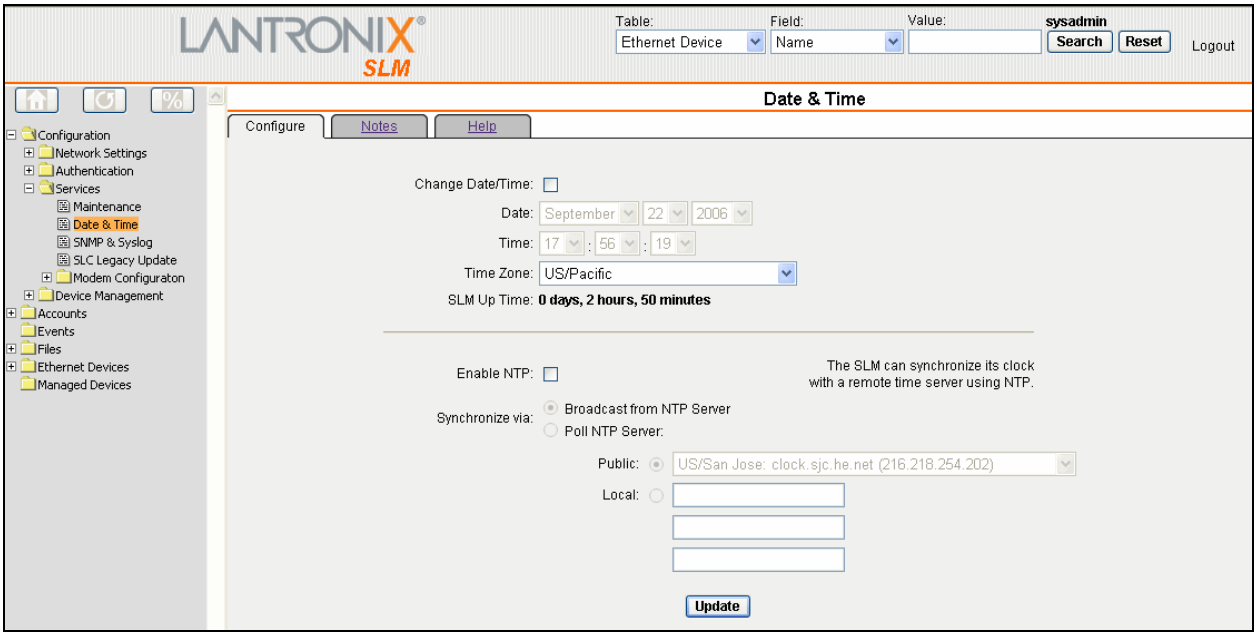
Date and Time

You can specify the current date, time, and time zone at the SLM's location, or the SLM can use NTP to synchronize with an NTP server on your network.

To set the local date, time, and time zone:

1. On the menu, click **Configuration→Services→Date & Time**. The following page opens:

Figure 10-15. Date & Time Page



2. Enter the following information:Date and Time

Change Date/Time	Select the check box to manually enter the date and time at the SLM's location.
Date	From the drop-down lists, select the current month, day, and year.
Time	From the drop-down lists, select the current hour and minute.
Time Zone	From the drop-down list, select the appropriate time zone.
SLM Up Time	Indicates how long the SLM has been up and running.

3. To save, click the **Update** button. When the update is complete, a confirmation message displays.

To synchronize the SLM with a remote timeserver using NTP:

1. Enter the following:

Enable NTP	Select the check box to enable NTP synchronization. NTP is disabled by default.
Synchronize via	Select one of the following: **Broadcast from NTP Server:** Enables the SLM to accept time information periodically transmitted by the NTP server. This is the default if you enable NTP. **Poll NTP Server:** Enables the SLM to query the NTP Server for the correct time. If you select this option, complete one of the following: ***Local:*** Select this option if the NTP server is on a local network, and enter the IP address of the NTP server. This is the default, and we highly recommend it. ***Public:*** Select this option if you want to use a public NTP server, and select the address of the NTP server from the drop-down list. We do not recommend this because of the high load on many public NTP servers. All servers in the drop-down list are stratum-2 servers. (See www.ntp.org for more information.)

2. To save, click the **Update** button. When the update is complete, a confirmation message displays.

Date and Time Commands

set datetime

Syntax

```
set datetime <one parameter>
```

Parameters

```
date <MMDDYYhhmm[ss]>
timezone <Time Zone>
```

Description

Sets the local date, time, and time zone (one parameter at a time).

Note: *If you type an invalid time zone, the system guides you through the process of selecting a time zone.*

show datetime

Syntax

```
show datetime
```

Description

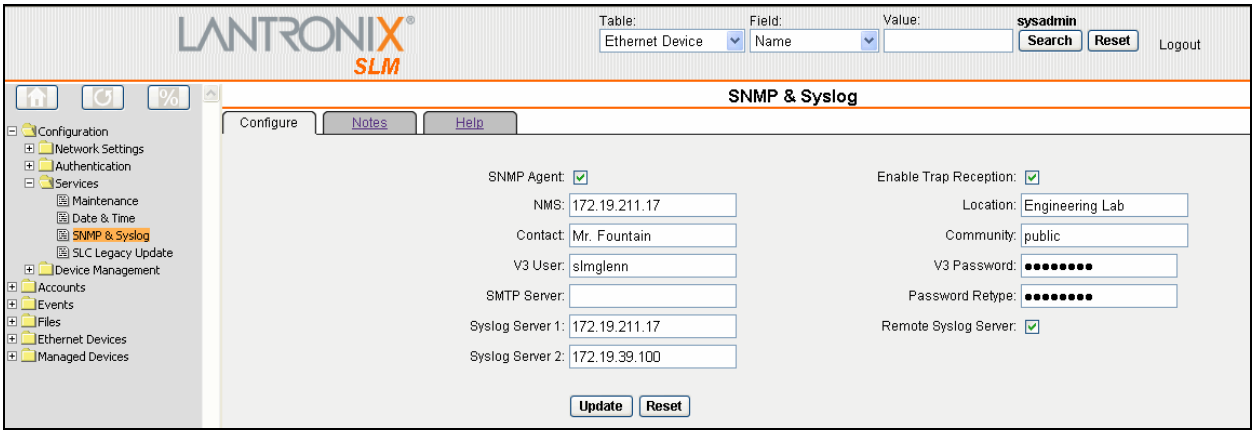
Displays the local date, time, and time zone.

SNMP & Syslog

Administrators can configure a Simple Network Management Protocol (SNMP) agent to allow users read-only access to the system.

1. On the menu, click **Configuration→Services→SNMP Agent**. The following page opens:

Figure 10-16. SNMP& Syslog Page



2. Enter the following information:

SNMP Agent	Enables read-only access into the SLM. Disabled by default.

Enable Trap Reception	Enables the SLM to receive traps from outside and to store and display them on the Traps page. Disabled by default. Traps are notifications of certain critical events. This feature is applicable when SNMP is enabled. When the SLC or other SecureLinx product (SLM, SLP, or SLK) configures the SLM as its NMS, the SLM receives these traps and displays them on the Traps page. The Traps page display has three levels: Level 1: Ethernet device Level 2: SLM/SLC/SLP/SLK Level 3: Individual device page
NMS	When SNMP is enabled, an NMS acts as a central server, requesting and receiving SNMP-type information from any computer using SNMP. The NMS can request information from the SLM and receive traps from the SLM. Enter the IP address of the NMS server. Required if you selected **SNMP Agent**.
Location (optional)	Physical location of the SLM. Useful for managing the SLM using SNMP.
Contact (optional)	Description of the person responsible for maintaining the SLM, for example, a name.
Community	Acts as an authentication key for other devices requesting SNMP MIB information from the SLM. Defaults to **public.**
V3 User	SNMP v3 is secure and requires user-based authorization to access SLM MIB objects. Enter a user name. No defaults.
V3 Password and **Password Retype**	Password for accessing the SNMP v3. No defaults.
SMTP Server	IP address of your network's Simple Mail Transfer Protocol (SMTP) relay server.
Syslog Server 1 and Syslog Server 2	IP addresses of the main and secondary servers to which the SLM system logs are being forwarded.
Remote Syslog Server	Select to indicate that the SLM will act as a remote syslog server to receive syslogs from other Ethernet devices (devices that have the SLM's IP Address specified as that device's syslog server).

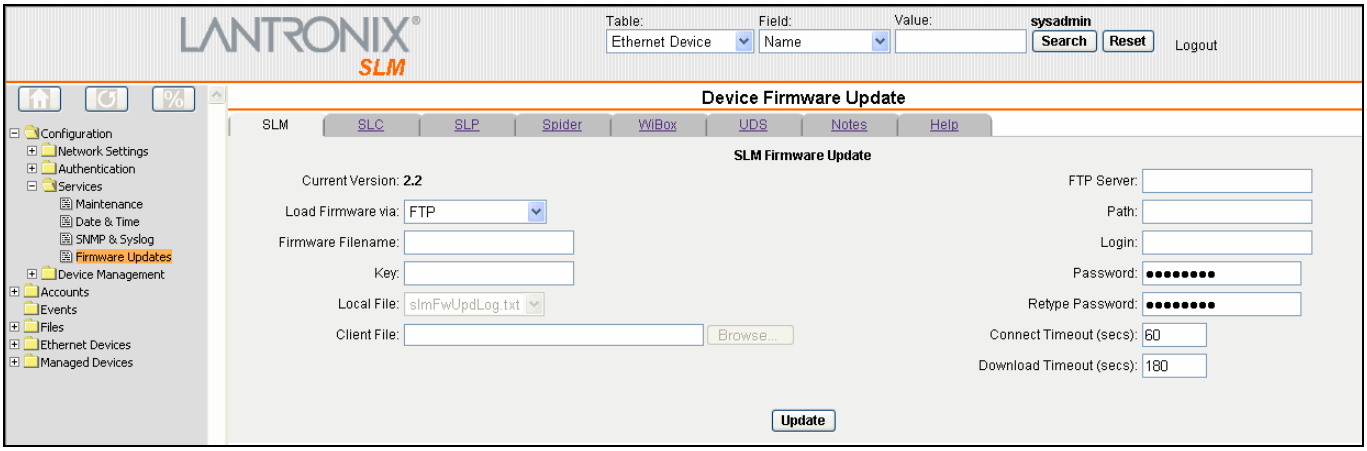
3. To save, click the **Update** button. When the update is complete, a confirmation message displays.

Device Firmware Updates

On these pages, you can update the firmware of Lantronix's Ethernet Devices.

1. On the main menu, click **Services→Firmware Updates**. The following page opens:

Figure 10-17. Device Firmware Update Page – SLM Tab



SLM Firmware

To update SLM firmware:

1. Enter the following information:

Current Version (view only)	Number of the firmware release on the SLM
Load Firmware via	From the drop-down list, select the method of loading the firmware. Options are **FTP, SFTP,** and **Local File**. FTP is the default. ***Note:*** *The Local File option is active only when at least one file exists in the SLM FW Upgrade Files directory.*
Firmware Filename	The name of the firmware update file downloaded from the Lantronix web site.
Key	If the user selects the firmware file from the SLM FW Upgrade Files directory, no entry is required. Otherwise, enter a key for validating the firmware file. Lantronix provides the key with the firmware file (32 hex characters).
Local File	From the drop-down list, select the firmware update (from the Files > SLM Upgrade Files directory).
Client File	Enter or browse to the file where the update is stored.
Check Lantronix (Only displays for service plan holders)	If you have an active Lantronix service plan for your SLM, you can download update files directly from the Lantronix server onto your SLM. If you select this checkbox, and click the **Submit** button, the SLM will interrogate the Lantronix Server to see if a firmware update file is available for your system. If one is present, then an additional option, **Lantronix Server**, displays in the **Load Firmware via** drop-down list.

FTP/SFTP Server

FTP Server	The IP address or host name of the server used for obtaining updates. May have up to 64 alphanumeric characters and may include hyphens and underscores.
Path	The default path on the server for obtaining firmware update files. May be blank.
Login	The user name for accessing the FTP server.
Password and **Confirm Password**	The FTP user password.
Connect Timeout (secs)	The number of seconds after which the connection attempt times out. Default is **60**.
Download Timeout (secs)	The number of seconds after which the download attempt times out. Default is **180**.

2. Click the **Update** button.

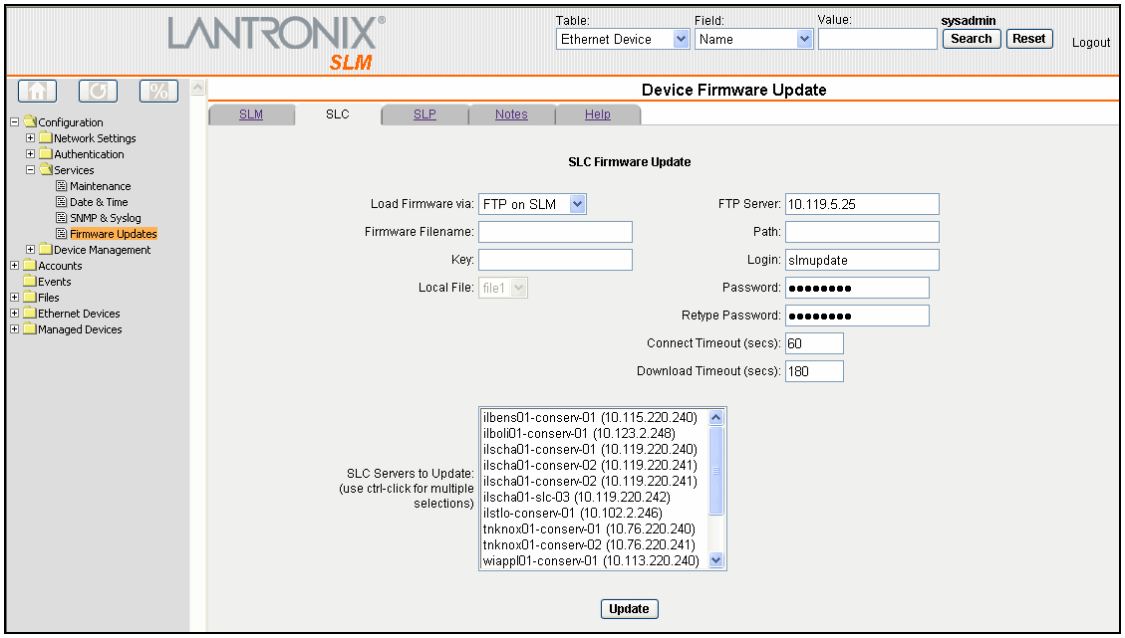
Note: *To check the progress of the update, click the* ***Progress*** *icon* *above the menu.*

SLC Firmware

To update SLC firmware:

1. On the Device Firmware Updates page, click the **SLC** tab. The following page opens:

Figure 10-18. Device Firmware Update Page -- SLC Tab



2. Enter the following information:

Load Firmware via	From the drop-down list, select the method of loading the firmware. You have the following options: **FTP on SLC, SFTP on SLC, and TFTP on SLC:** The SLM commands the SLC to download the SLC firmware file directly from a server to the SLC. **FTP on SLM and SFTP on SLM:** The SLM first checks to see whether the SLM firmware file already exists on the SLM local hard disk. If not, the SLM downloads it using FTP or SFTP. The SLM stores the firmware file locally, securely copies the file to the selected SLCs, and runs the firmware update on the SLCs. **HTTP From Client** *Note: The **Local File** option is active only when at least one file exists in the SLC FW Upgrade Files directory.*
Firmware Filename	The name of the firmware update file downloaded from the Lantronix web site.
Key	If the user selects the firmware file from the SLC FW Upgrade Files directory, no entry is required. Otherwise, enter a key for validating the firmware file. Lantronix provides the key with the firmware file (32 hex characters).
Local File	From the drop-down list, select the firmware update (from the Files > SLC Upgrade Files directory.)
Client File	Enter or browse to the file where the update is stored.

FTP/SFTP Server

FTP Server	The IP address or host name of the server used for obtaining updates. May have up to 64 alphanumeric characters and may include hyphens and underscores.
Path	The default path on the server for obtaining firmware update files. May be blank.
Login	The user name for accessing the FTP server.
Password and **Confirm Password**	The FTP user password.
Connect Timeout (secs)	The number of seconds after which the connection attempt times out. Default is **60**.
Download Timeout (secs)	The number of seconds after which the download attempt times out. Default is **180**.

3. In the **SLC Servers to Update** area, select one or more of the SLCs managed by the SLM. (Use **Ctrl+click** for multiple selections.)
4. To update the SLCs, click the **Update** button. When the update is complete, a confirmation message displays.

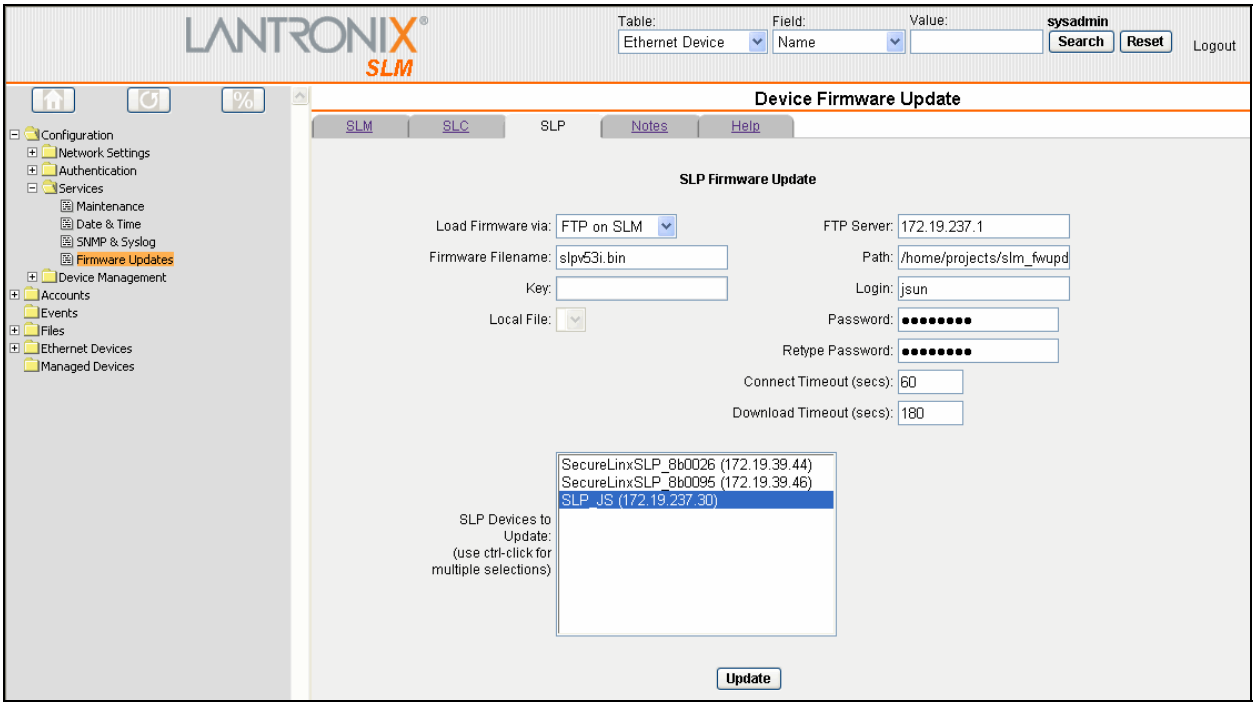
*Note: To check the progress of the update, click the **Progress** icon above the menu.*

SLP Firmware

To update SLP firmware:

1. On the Device Firmware Update page, click the **SLP** tab. The following page opens:

Figure 10-19. Device Firmware Update – SLP Tab



2. Enter the following information:

Load Firmware via	From the drop-down list, select the method of loading the firmware. You have the following options: **Select FTP on SLP** for the SLM to command the SLP to download the SLP firmware file to the SLP directly from a server. **Select FTP on SLM or SFTP on SLM** for the SLM to first check to see whether the SLP firmware file already exists on the SLM local hard disk. If not, the SLM downloads it using FTP or SFTP. The SLM stores the firmware file locally; then the SLM serves as the FTP server and allows the SLP to download the firmware file from the SLM, and then runs the firmware update. **HTTP From Client** *Note: The **Local File** option is active only when at least one file exists in the SLP FW Upgrade Files directory.*
Firmware Filename	The name of the firmware update file downloaded from the Lantronix web site.

Key	If the user selects the firmware file from the SLP FW Upgrade Files directory, no entry is required. Otherwise, enter a key for validating the firmware file. Lantronix provides the key with the firmware file (32 hex characters).
Local File	From the drop-down list, select the firmware update (from the **Files > SLP Upgrade Files** directory.)

FTP/SFTP Server

FTP Server	The IP address or host name of the server used for obtaining updates. May have up to 64 alphanumeric characters and may include hyphens and underscores.
Path	The default path on the server for obtaining firmware update files. May be blank.
Login	The user name for accessing the FTP server.
Password and **Confirm Password**	The FTP user password.
Connect Timeout (secs)	The number of seconds after which the connection attempt times out. Default is **60**.
Download Timeout (secs)	The number of seconds after which the download attempt times out. Default is **180**.

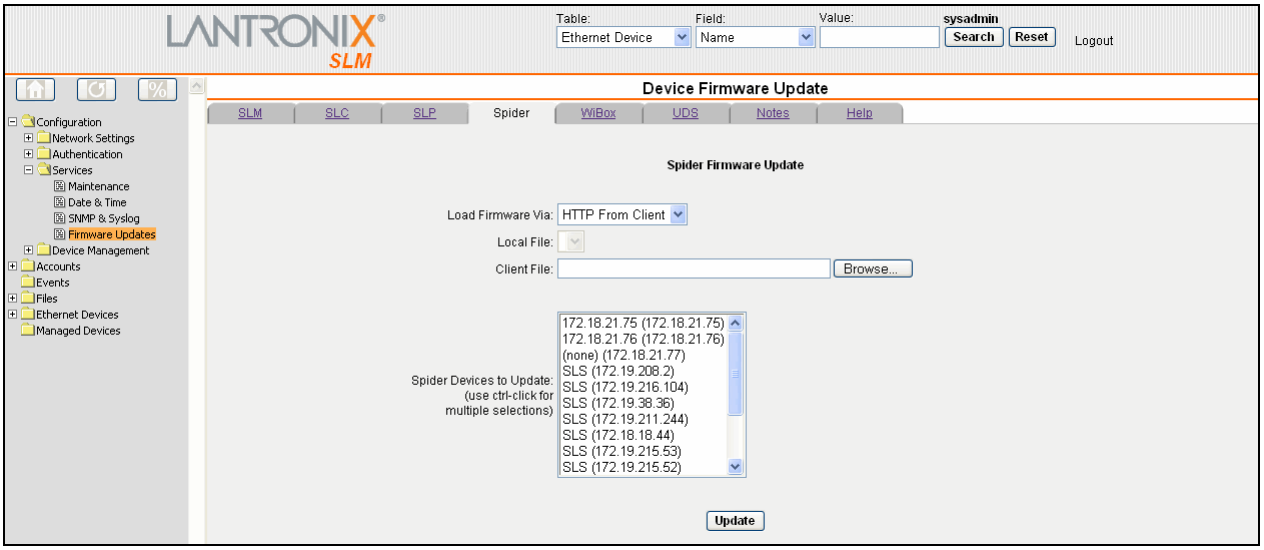
3. In the **SLP Servers to Update** area, select one or more of the SLPs managed by the SLM. (Use **Ctrl+click** for multiple selections.)
4. To update the SLPs, click the **Update** button. When the update is complete, a confirmation message displays.

*Note: To check the progress of the update, click the **Progress** icon* *above the menu.*

Spider Firmware

1. On the Device Firmware Updates page, click the **Spider** tab. The following page opens.

Figure 10-20. Device Firmware Update Page – Spider Tab



2. Enter the following information:

Load Firmware via	From the drop-down list, select the method of loading the firmware. You have the following options: **HTTP From Client** ***Note:*** *The Local File option is active only when at least one file exists in the Spider FW Upgrade Files directory.*
Local File	From the drop-down list, select the firmware update file stored on the SLM.
Client File	Enter or browse to the file where the update is stored.

3. In the **Spider Devices to Update** area, select one or more of the Spiders the SLM is managing. (Use **Ctrl+click** for multiple selections.)
4. To update the Spiders, click the **Update** button. When the update is complete, a confirmation message displays.

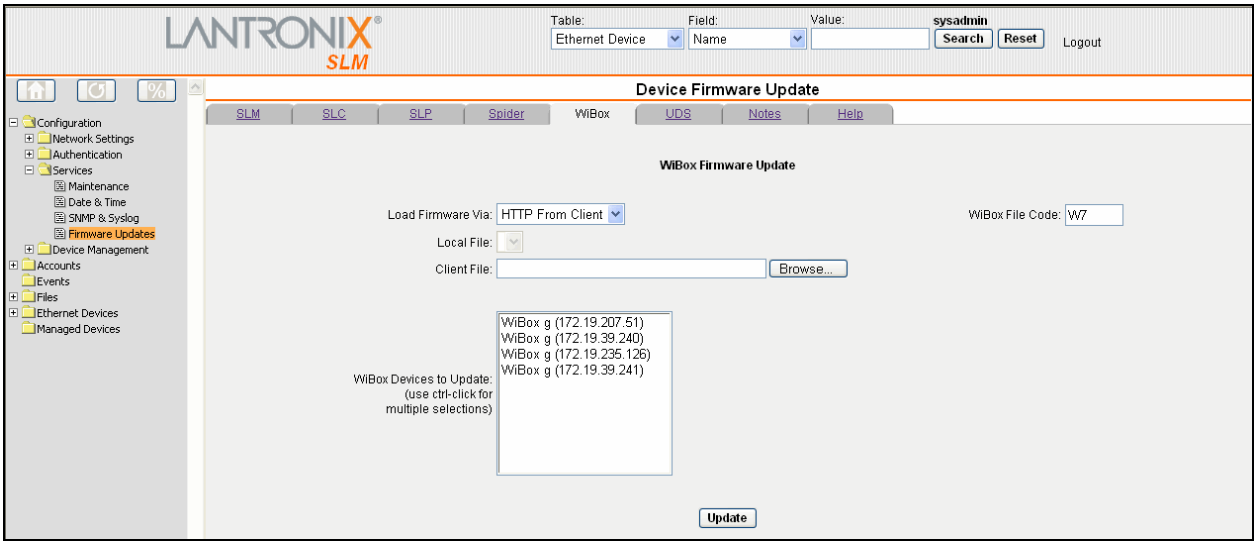
Note: *To check the progress of the update, click the* ***Progress*** *icon* *above the menu.*

WiBox Firmware

To update firmware on a WiBox:

1. On the Device Firmware Updates page, click the **WiBox** tab.

Figure 10-21. Device Firmware Update Page – WiBox Tab



2. Enter the following information:

Load Firmware via	From the drop-down list, select the method of loading the firmware. You have the following options: **HTTP From Client** ***Note:*** *The Local File option is active only when at least one file exists in the WiBox FW Upgrade Files directory.*
Local File	From the drop-down list, select the firmware update file stored on the SLM.
Client File	Enter or browse to the file where the update is stored.
WiBox File Code	*Enter the 2-character firmware code that matches your WiBox.* ***Note:*** *Not all WiBox units share the same code. See the User Guide for your WiBox to find the correct code.*

3. In the **WiBox Devices to Update** area, select one or more of the WiBoxes the SLM is managing. (Use **Ctrl+click** for multiple selections.)
4. To update the WiBoxes, click the **Update** button. When the update is complete, a confirmation message displays.

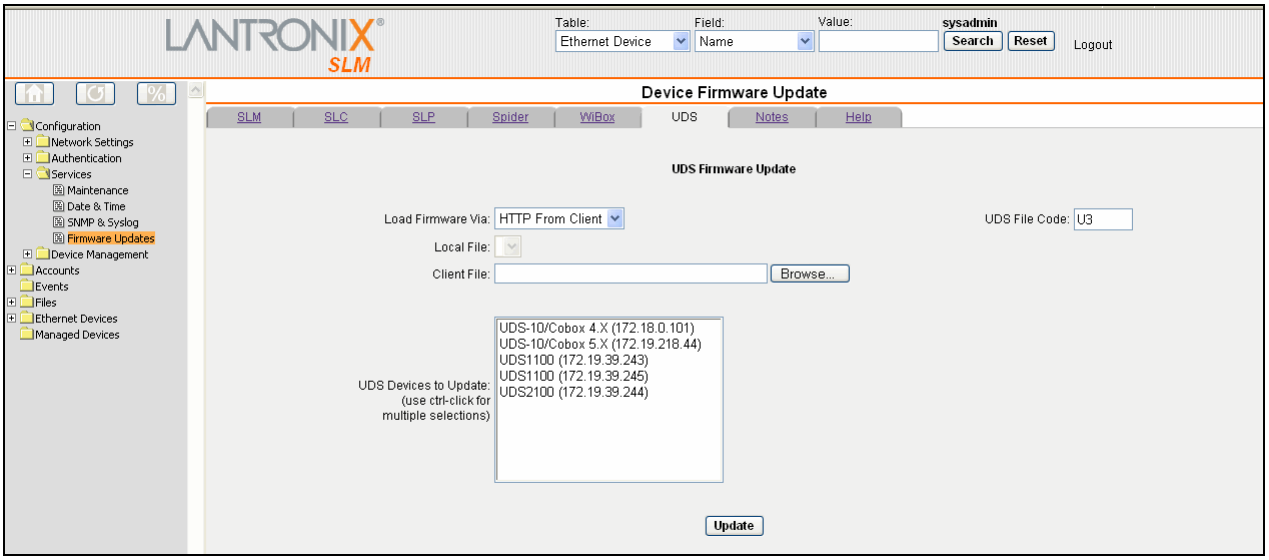
Note: *To check the progress of the update, click the* ***Progress*** *icon above the menu.*

UDS Firmware Updates

To update firmware on a UDS:

1. On the Device Firmware Updates page, click the **UDS** tab. The following page opens:

Figure 10-22. Firmware Update Page – UDS Tab



2. Enter the following information:

Load Firmware via	From the drop-down list, select the method of loading the firmware. You have the following options: **HTTP From Client** ***Note:*** *The Local File option is active only when at least one file exists in the UDS FW Upgrade Files directory.*
Local File	From the drop-down list, select the firmware update file stored on the SLM.
Client File	Enter or browse to the file where the update is stored.
WiBox File Code	*Enter the 2-character firmware code that matches your UDS.* ***Note:*** *Not all UDS units share the same code. See the User Guide for your UDS to find the correct code.*

3. In the **UDS Devices to Update** area, select one or more of the UDS units the SLM is managing. (Use **Ctrl+click** for multiple selections.)
4. To update the UDS units, click the **Update** button. When the update is complete, a confirmation message displays.

Note: *To check the progress of the update, click the* ***Progress*** *icon above the menu.*

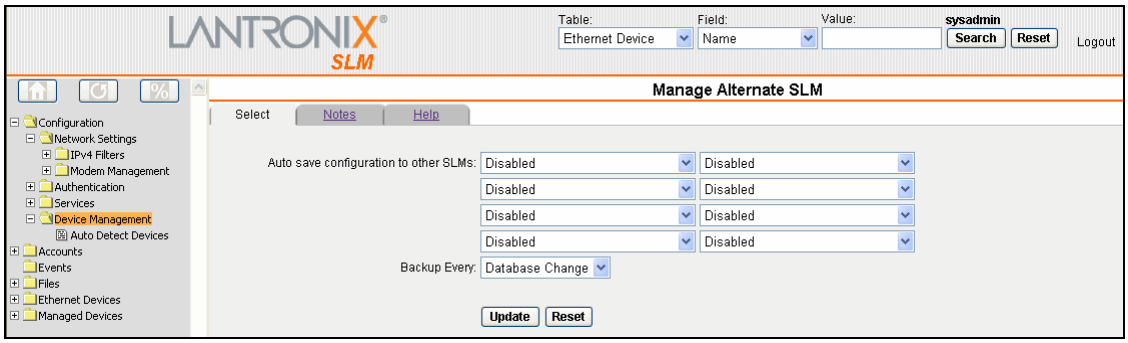
Managing Alternate SLMs

When **Auto save configuration to other SLMs** is enabled, the SLM immediately saves its own configuration to up to eight remote SLMs. After that, every time the SLM configuration has changed, it waits 60 minutes to make sure there are no more changes before saving another configuration to the remote SLMs. The remote SLMs keep the most recent 10 configuration files saved by auto save configuration.

To auto-save a configuration:

1. On the menu, click **Configuration→Device Management**. The following page opens:

Figure 10-23. Auto Saving a Configuration



2. Enter the following information:

Auto save configuration to other SLMs	From the drop-down lists, select up to eight SLMs on which automatically saved configuration files will be stored. (Disabled by default.) ***Note:*** *For SLMs to populate the drop-down lists, they must have a secure channel connection with your SLM.*
Backup Every	From the drop-down list, select how often to back up the configuration(s). You can back up the configuration(s) every time there is a database change or at specific daily intervals, regardless of whether there was a change.

3. To save, click the **Update** button. When the update is complete, a confirmation message displays.
4. To reset to original values, click the **Reset** button.

Managing SLCs

Administrators can reboot or shutdown SLCs, update SLC firmware, get log, status, and configuration files, restore configurations, and execute CLI commands.

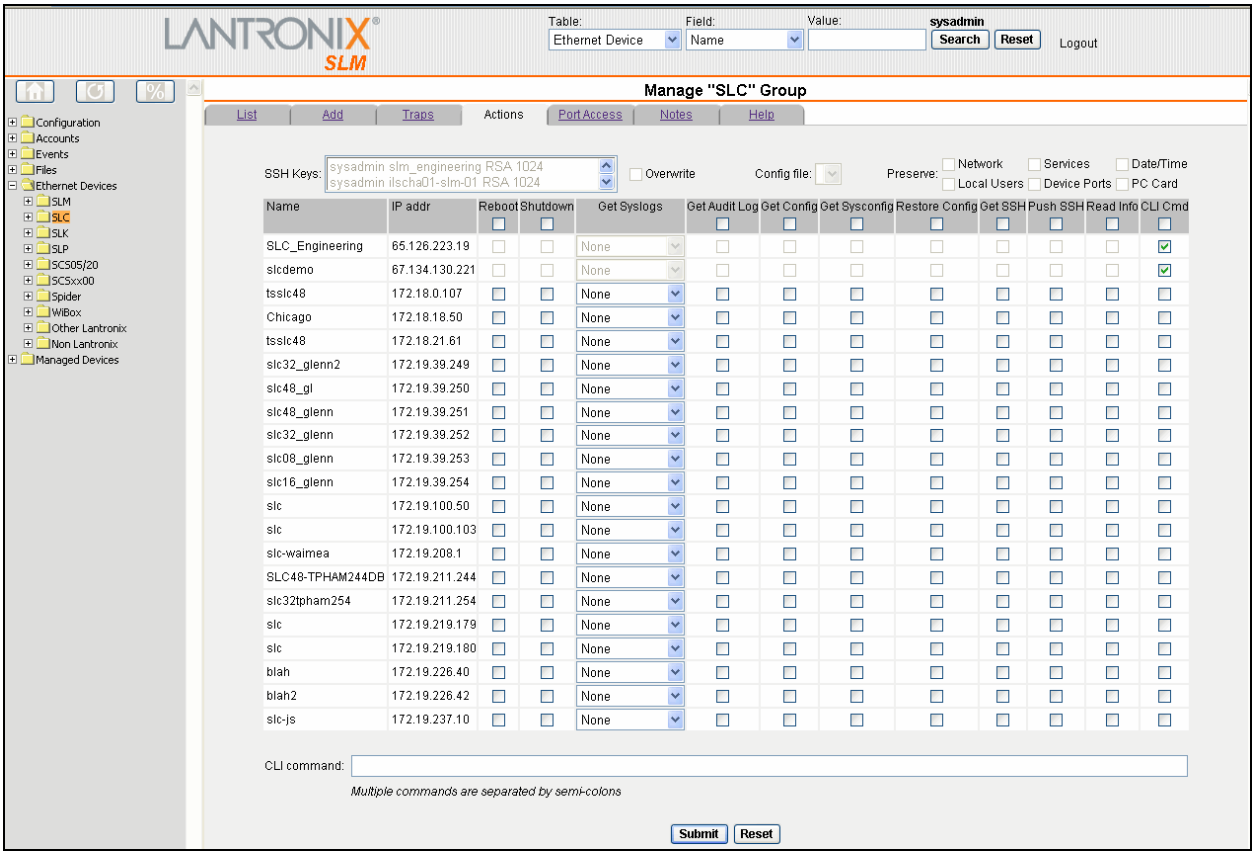
Using the Actions Tab

The **Actions** tab of the Manage "SLC" Group and Manage "SLB" Group page allows you to perform many tasks related to the discovered SLCs/SLBs. You can perform only one action at a time on a single SLC/SLB, but you may perform the same action on multiple or all SLCs/SLBs or different actions on multiple SLCs/SLBs.

1. On the menu, click **Ethernet devices→SLC**. The Manage "SLC" Group page opens.

2. Click the **Actions** tab. The following page opens:

Figure 10-24. Manage "SLC" Group Actions Tab



3. To perform an action on all of the listed SLCs, select the check box in the column header,

   OR

   To perform an action on multiple SLCs, select the check box for each desired SLC.

   Before performing an action on another group of devices, access the SLM auditlog or SLM syslog file.

   Following are the available actions:

   - Reboot
   - Shutdown
   - Get Syslogs
   - Get Audit Log
   - Get Config
   - Get Sysconfig
   - Restore Config
   - Get SSH/Push SSH
   - Read Info
   - CLI Cmd (For CLI Cmd, you may specify any number of devices.)

4. Click the **Progress** icon to view the status of your commands. For more details, view the SLM auditlog and SLM syslog.

Rebooting or Shutting Down

Use the **Actions** tab to reboot or shut down one or more SLCs.

To reboot or shut down:

1. To reboot an SLC, select the **Reboot** check box for the SLC,

   OR

   To shut down an SLC, select the **Shutdown** check box for the SLC.

2. Click the **Submit** button.

Getting a Log File

Use the **Actions** tab to get a syslog or audit log file from one or more SLCs.

Notes:

- *The SLM stores files in the Files directories. You can display a file from the appropriate Files directory.*
- *The file name format is*

  [first 8 characters of SLC host name] _[last 8 characters of MAC Address]-YYMMDD_hhmm-[type of logfile].

  For example, the syslog file retrieved from SLC 'slc32glenn2' (MAC address: 00:11:11:00:11:11) at 15:11 Nov 2, 2006 is

  'slc32gle_11001111-061102_1511-slcsyslog'.

To get a syslog or audit log file from an SLC:

1. To get the syslog from an SLC, select the type of syslog from the **Get Syslogs** drop-down list,

   OR

   To get the audit log from an SLC, select the **Get Audit Log** check box for the SLC.

2. Click the **Submit** button.

Getting or Restoring a Configuration File

Use the **Actions** tab to get a specific configuration file from one or more SLCs or to restore a configuration to one or more SLCs.

Note: *The SLM stores files in the Files directories. You can display a file from the appropriate Files directory.*

To get a configuration file from an SLC:

1. Select the **Get Config** check box for the SLC.
2. Click the **Submit** button.

To restore a configuration to an SLC:

1. From the **Config file** drop-down list at the top of the page, select the desired configuration file.
2. Select the **Restore Config** check box for the SLC.

3. Select the **Preserve** check boxes to retain the current configuration parameters after the configuration is restored. You may make multiple selections. (Options are **Network**, **Services**, **Date/Time**, **Local Users**, **Device Ports**, and **PC Care**.)
4. Click the **Submit** button.

Getting a Sysconfig File

Use the **Actions** tab to get a sysconfig file from one or more SLCs.

To get a sysconfig (system status) file:

1. Select the **Get Sysconfig** check box for the SLC.
2. Click the **Submit** button.

Getting or Pushing SSH Keys

Use the **Actions** tab to retrieve or export SSH keys from or to one or more SLCs.

Note: *To view SSH keys, click **Configuration->Authentication->SSH Keys** on the menu, and then click the **SLC Keys** tab.*

Get SSH key retrieves all the imported public SSH keys from the selected SLC and stores them in the database. **Push SSH key** exports the selected SSH keys to the selected SLCs.

When an SLC imports a public key (with a specific user and host name) from a host (could be an SLM or another PC), this SLC allows that particular user to access the SLC from that particular host. When you enable **Get SSH** keys from an SLC, the SLM retrieves all the imported public keys from that particular SLC and stores them in the SLM database. Then you can push those public keys retrieved from one SLC to other SLCs, allowing those particular users to access other SLCs from those particular hosts.

To get SSH keys:

Example: Following is an example of how the user may get and push SSH Keys.

SLC-1 has three imported public keys:

key1: user-A@host-X

key2: user-B@host-Y

key3: user-C@host-Z

The user enables **Get SSH key** from SLC-1 on the SLM. As a result, the SLM database has the three keys above.

The user selects key1 and key3 on the SLC **Actions** tab on the SLM and enables **Push SSH Key** to SLC-20 and SLC-21.

Now SLC-20 and SLC-21 have both key1 and key3. This means that SLC-20 and SLC-21 allow user-A to access them from host-X, and allow user-C to access them from host-Z.

To push SSH keys:

1. To overwrite SSH keys with the same host and user name currently in the database, select the **Overwrite** check box at the top of the page.
2. Select the **Get SSH** check box for the SLC.
3. Click the **Submit** button.

To push SSH keys:

1. To overwrite SSH keys with same user name and host name on the SLC where you are exporting the SSH, select the **Overwrite** check box at the top of the page.
2. Select the **Push SSH** check box for the SLC.
3. Click the **Submit** button.

Reading Information

Use the **Actions** tab to update the SLM's database with SLC device and port information.

To read information from SLCs:

1. Select the checkboxes for the SLCs to read.
2. Click the **Submit** button.

Note: *This is the same as the **Read info from devices** check box on the SLC device page. On the **Actions** page, you can issue this action for multiple SLC devices at once.*

Issuing a CLI Command

Use the **Actions** tab to issue a CLI command to one or more SLCs.

Note: *Commands issued from the **Actions** tab are not interactive.*

The following command will not work, because the SLC CLI requires confirmation to continue with group configuration commands:

```
set device port 1-3 baud 19200
```

The following commands will not work, because the SLC CLI requires confirmation to continue with admin maintenance configuration commands:

```
admin reboot
admin shutdown
admin config
```

The following commands will not work because the SLC CLI does not send status “settings successfully updated”, which lets the SLM know that the command was successful:

```
show [anything]
```

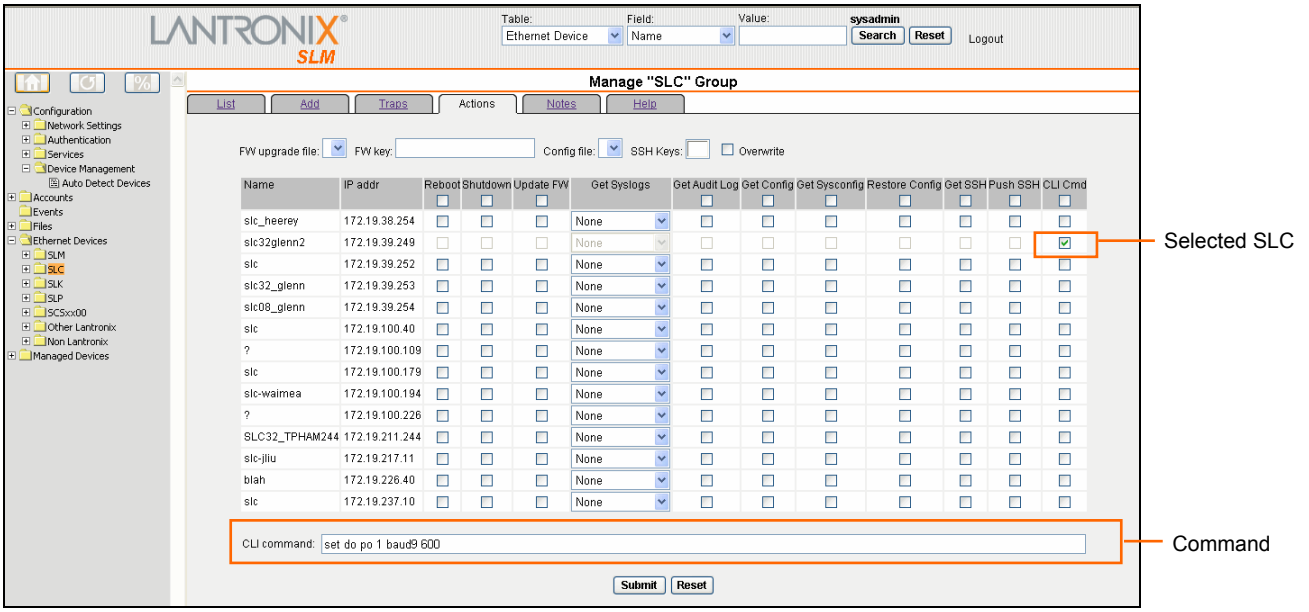
Examples of commands that do work are:

```
se de po 1 baud 9600
set cli terminallines disable
```

To issue a CLI command:

1. Select the **CLI Cmd** check box for the SLC.

Figure 10-25. Issuing a CLI Command



2. In the **CLI command** field at the bottom of the page, enter the command. You can issue multiple commands, separated by semicolons (;).
3. Click the **Submit** button.

Viewing Progress of Update FW and CLI Commands

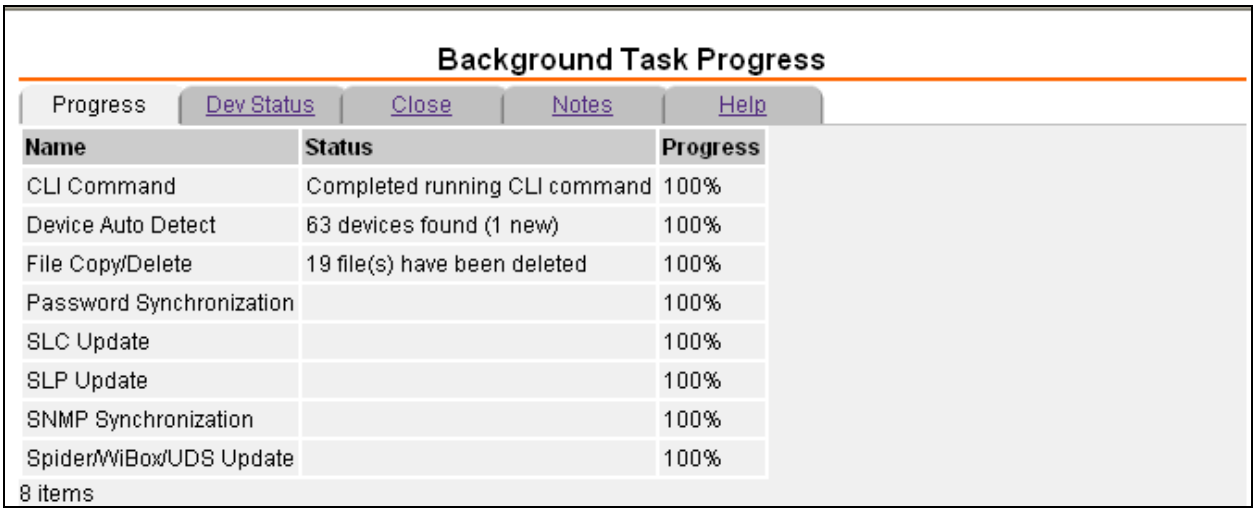
You use the **Progress** button to view the progress of the **Update FW** and **CLI CMD** actions described above.

Note: *For more detailed status, view the SLM auditlog in the Files folder.*

To view the progress of actions running in the background:

1. Click the **Progress** icon The following page opens:

Figure 10-26. Background Task Progress Page – Progress Tab

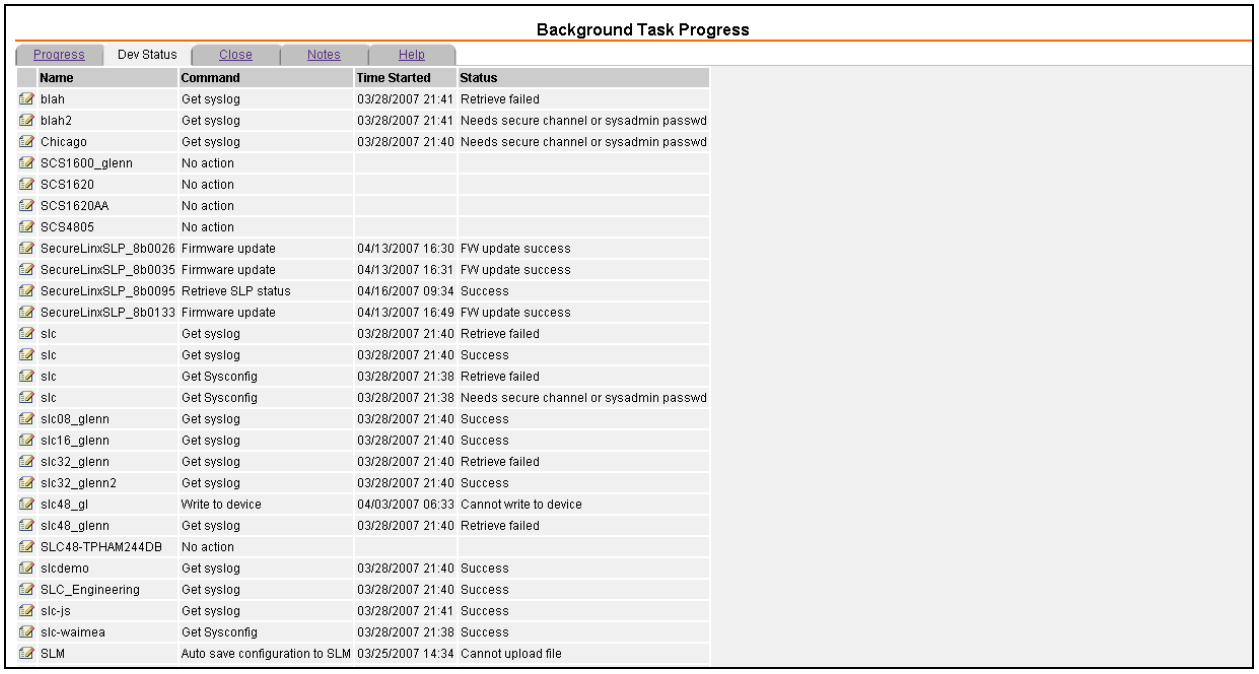


2. View the following information about each task.

Name	Name of the task.
Status	Informational text.
Progress	Percentage of the task that is complete.

3. To view details of the last device action status of the SLMs/SLCs/SLPs/SCS, click the **Dev. Status** tab. The following page opens:

Figure 10-27. Background Task Progress – Dev Status Tab



To close the Background Task Progress page, click the **Close** tab.

Events

Administrators can configure alarms, triggers, and events on the SLM. Examples of events are receiving an SNMP trap, a system event like network failure, or a text string match in a certain log. There are several types of logs in the SLM system: data logs (device port buffering), syslogs, event logs, access logs (user access), and audit logs. The alarm could send an email to a user, send an SNMP trap, or write to a log file (local syslog or remote syslog).

Event Management

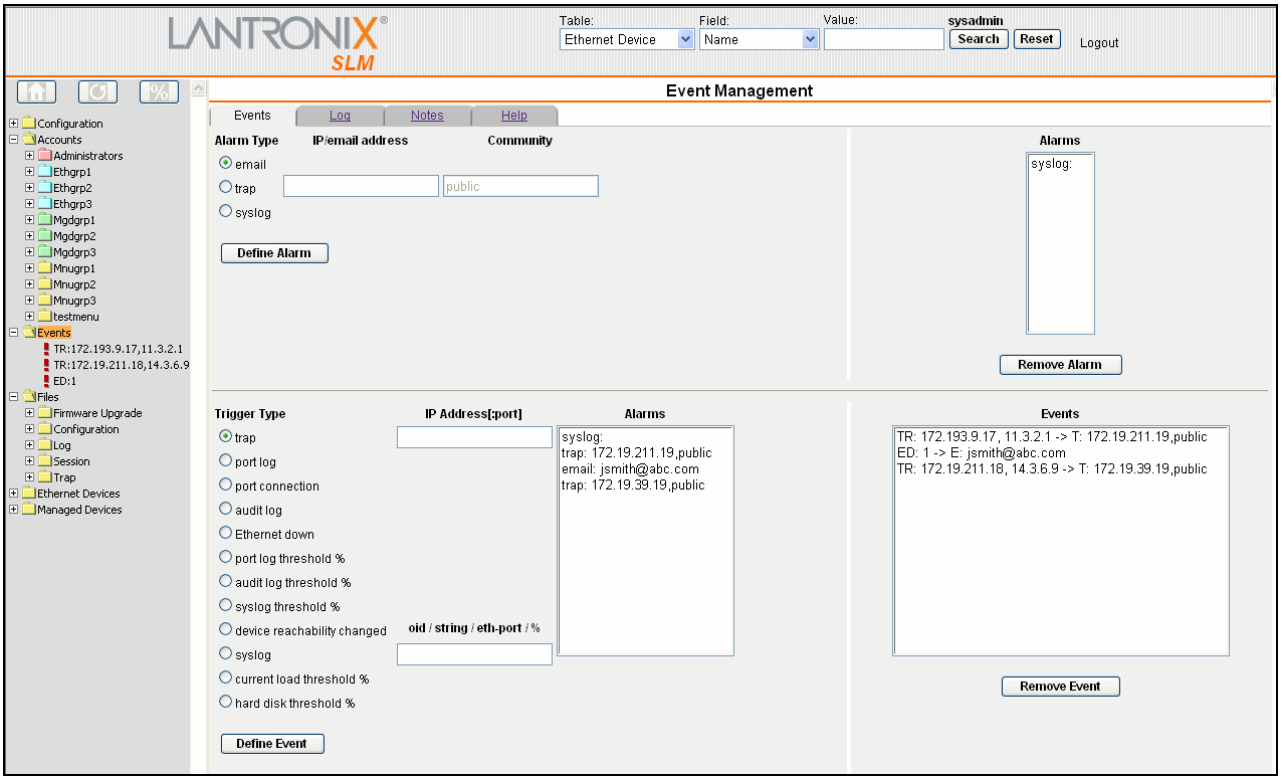
Administrators configure alarms and triggers. An alarm is a notification that may take the form of an email, trap, or syslog. A trigger is something that happens to set off an alarm assigned to that trigger. An event is a combination of a trigger and an alarm.

You can map one trigger to multiple alarms and/or multiple triggers to one alarm (saving you from having to define the same alarm repeatedly for each trigger).

To define alarms:

1. On the menu, click **Events**. The following page opens:

Figure 10-28. Event Management Page – Events Tab



2. Enter the following information:

Alarm Type

Alarm Type	Select one of the following: **email:** Sends an email to the specified email address with details of the event that has been triggered. **trap:** Sends a notification of a critical event to a specified IP address. **syslog:** Writes an entry into the syslog with details of the event.
IP/email address	**For an Email alarm:** The email address where notifications go. **For a trap:** The IP address of the device to which notifications go. **For a syslog**: Leave blank.
Community	**For a trap:** The SNMP community of the device to which the trap is sent. The default is **public**. **Example:** If the alarm type is **Trap**, and the IP address is 172.19.100.123, the SNMP community name should be the SNMP community of the device 172.19.100.123. Otherwise the device will not receive the trap.

3. Click the **Define Alarm** button. The alarm displays in the **Alarm** list on the right.
4. Enter the following information:

Trigger Type

Trigger Type	Select one of the following: **trap:** An incoming trap from a specified IP address. **port log:** A defined string matches a monitored device's port log. The string match for the port log could be either an exact string match, or a regular expression. See the **string** field for an example. **port connection:** A defined string matches a monitored device's port connection. **audit log:** A defined string matches an entry in the audit log. **Ethernet down:** A defined ethernet port has failed (for example, eth-port: 2). **port log threshold %:** The SLC port log files have reached a defined percentage of the SLC Portlog directory's capacity. **audit log threshold %**: The **SLM** or **SLC** audit log files have reached a defined percentage of the SLM Auditlog directory's capacity. **syslog threshold %:** The **SLM** or **SLC** syslog files have reached a defined percentage of the SLM Syslog directory's capacity. **device reachability changed:** If you specify the device's IP Address with this trigger type, the SLM sets the trigger should polling fail on this device. If you do not specify the device's IP Address, the SLM sets the trigger on all the devices on which polling failed. When polling is enabled on a device (the **Poll** check box on the device page), the SLM constantly checks on the device to see if that device is reachable. **Syslog:** Enter the text string for the string match in the **oid / string / eth-port / %** field. This is the trigger when a syslog string matches the specified string. This is a very powerful trigger because the SLM can act as a syslog server by receiving a syslog from SLCs and other devices. You can do a string match to all kinds of syslog messages (e.g., for all SLC events that will send a message to syslog). **current load threshold %:** Enter the IP address and port number (optional) of the SLP or SLB you want to monitor and its current load threshold %. If you specify a port number, the trigger is set when the current load (**outletLoad)** of the outlet # (port #)

	reaches the **outletLoad** theshold on that particular SLP or SLB. If you do not specify a port number, the trigger is set when the current load (infeedLoad) of the whole SLP or SLB reaches the infeedLoad threshold. **hard disk threshold %:** Enter the percentage of the hard disk threshold of the SLM. The SLM sends out the alarm when the hard disk usage reaches this threshold.
IP Address[:port]	**For a trap, port log, or port connection:** Enter the IP address followed by an optional port number 1-48, for example, 172.19.39.19:15. ***Note:*** *The brackets indicate that: port is not always required.*
oid / string / eth-port /%	Depending on the trigger type selected, enter one or more of the following: **oid:** A unique identifier for an SNMP object. (An SNMP object is anything that can hold a value and can be read using an SNMP "get" action.) The OID consists of a string of numbers separated by periods (for example, 1.1.3.2.1). Each number is part of a group represented by the number on its left. **string:** Series of characters that match a monitored device's audit log, syslog, or port log. The OID string match supports partial match. The string match for a port log could be an exact string or a regular expression. For example: String "reboot" will match port logs containing "reboot." String "RE:abc[0-9]" will match port logs containing any string that matches the regular expression "abc[0-9]." OID .3.6.1.4.1.244.1.1 will match any SLC custom traps with OID: .3.6.1.4.1.244.1.1.0.1 to 1.3.6.1.4.1.244.1.1.0.4. **eth-port:** Ethernet port that is down (for example, 2). **%:** Defined percentage of the SLC port log file's capacity. ***Note:*** *For detailed instructions on completing the OID for a trap, see the Lantronix web site www.lantronix.com/support).*

5. In the **Alarms** list to the right, select the alarm(s) to be associated with the selected trigger.
6. Click the **Define Event** button. The event displays in the format Trigger: Alarm in the **Events** list on the page. The trigger displays in the **Events** menu tree.

Figure 10-29. SNMP Trap Configuration (Lantronix Tech Support FAQ)

LANTRONIX
Network anything. Network everything.™
Search
HOME PRODUCTS SOLUTIONS SUPPORT NEWS & EVENTS LEARNING CENTER PARTNERS ABOUT US HOW TO BUY
Support
Support
Technical FAQs
Online Tutorials
Cable / Adaptor Lookup
Questions
- Pre Sales
- Post Sales
Live Assist
Downloads
Utilities
Documentation
Product Bulletins
Novell NDS Registration
FTP Site
Feedback
Warranty Policy
Product Registration
Extended Support & Services
New Online Tutorials!
Check out the new MSS Tutorials on the Lantronix support site.
For more details, Click Here
Home > Support
Answers
Send an E-mail
My Stuff
Login
Help
Product
SLM
All Sub-Products
Search by Keyword
Search Tips?
event
Search
Search by
Phrases
Powered by RightNow
ID
1267
Product
SLM
Print Answer
E-mail Answer
SNMP trap configuration on an SLM
Question
How do I configure SNMP Trap Event Triggers on an SLM? Do I need to specify the full OID for every trap I want to use as a trigger?
Answer
This answer applies to SLM firmware v2.0 and higher.
On the SLM Events page, when you setup a "Trap" as an Event Trigger, you don't have to explicitly describe the OID down to the last digit.
Example 1:
If you define a trap as shown below:
Trigger Type
[v] Trap
IP Address: 172.19.237.10
OID: 1.3.6.1.4.1.244.1.1
It will match all SLC custom traps received from the specified IP address(172.19.237.10). These include:
1.3.6.1.4.1.244.1.1.0.1 (power supply)
1.3.6.1.4.1.244.1.1.0.2 (sysadmin password)
1.3.6.1.4.1.244.1.1.0.3 (shutdown)
1.3.6.1.4.1.244.1.1.0.4 (device port data)
Example 2:
If you define a trap as shown below:
Trigger Type
[v] Trap
IP Address: 172.19.237.10
OID: 1.3.6.1.6.3.1.1.5
It will match all generic SNMP traps received from the specified IP address(172.19.237.10). These include:
1.3.6.1.6.3.1.1.5.1 (cold start)
1.3.6.1.6.3.1.1.5.2 (warm start)
1.3.6.1.6.3.1.1.5.3 (link down)
1.3.6.1.6.3.1.1.5.4 (link up)
1.3.6.1.6.3.1.1.5.5 (auth failure)
1.3.6.1.6.3.1.1.5.6 (egpNeighborLoss)
Example 3:
If you define a trap as shown below:
Trigger Type
[v] Trap
IP Address: 172.19.237.10
OID: 1.3.6.1.4.1.244.1.1.0.1
This will only match SLC power supply trap received from the specified IP address(172.19.237.10).
Notify Me by E-mail if this Answer is Updated
How well did this answer your question?
100% 75% 50% 25% 0%
Submit Rating
Related Answers
Controlling how MSS products send data onto the network
MSS Products - SNMP Support - MIBs and Traps
CERT release regarding insecure implementations of the SNMP protocol
Configuring Events, Alarms and Notifications on an SLM
LPS1/MPS1/MPS100 - SNMP Support - MIBs and Traps
Back to Search Results
Embedded Ethernet / 802.11 | External Device Networking | Console Servers | Remote KVM
Remote Power Management | Terminal Servers | Print Servers | Video Extenders | Matrix Switches
Contact Us | Site Map | Terms of Use | Privacy | Copyright | RoHS / WEEE
Copyright © Lantronix, Inc. 2006. All rights reserved.

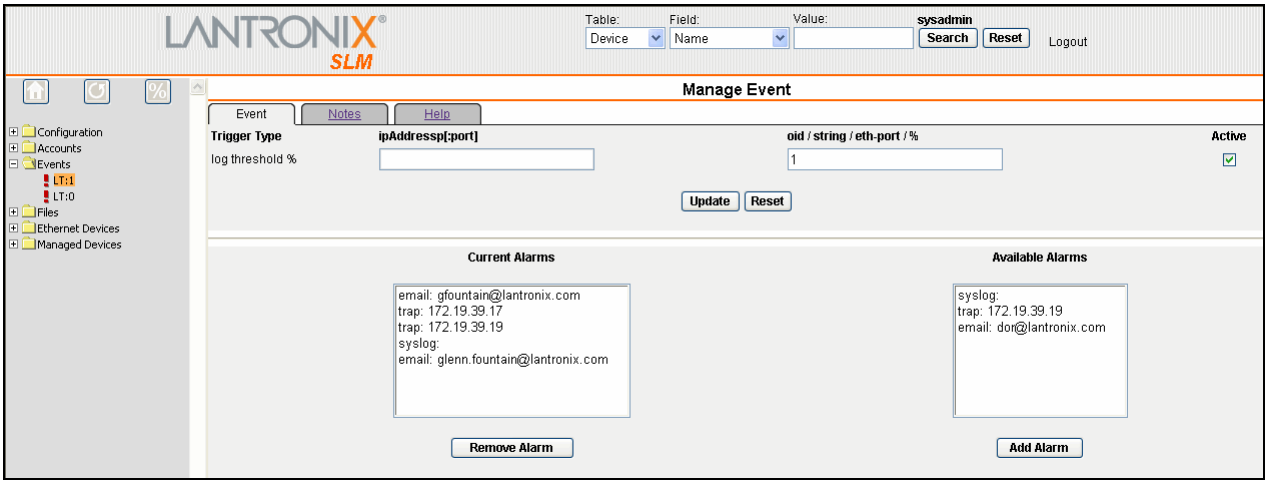
Updating and Deleting Events

Administrators and authorized users can update triggers and delete or add alarms for defined events.

To update information about the alarm, trigger, or event:

1. On the menu, open the **Events** menu tree and select the event to be managed. The following page opens:

Figure 10-30. Manage Event Page –Event Tab



2. Update the information about the alarm, trigger, or combination of alarm and trigger as desired.

   Note: *If you deactivate an event, it remains in the system but will not send alarms until it is reactivated.*

3. Click the **Update** button.

To add an additional alarm

You may add an alarm only if there are available alarms that are not already assigned to the trigger. You can add more alarms on the main Event Management page.

1. From the **Available Alarms** list, select another alarm.
2. Click the **Add Alarm** button. The alarm now displays in the **Current Alarms** list.

To delete an alarm:

On the Manage Event page you can remove an alarm only if there are more than two alarms to start with (you may not leave a trigger without an alarm).

1. Select the alarm from the **Current Alarms** list and click the **Remove Alarm** button. A confirmation message displays.
2. Click **OK**. The alarm is no longer in the **Alarms** list or in any events that use that alarm.

To delete an event:

1. Select the event from the **Events** list and click the **Remove Event** button. A confirmation message displays.
2. Click **OK**. The event is no longer in the **Events** list.

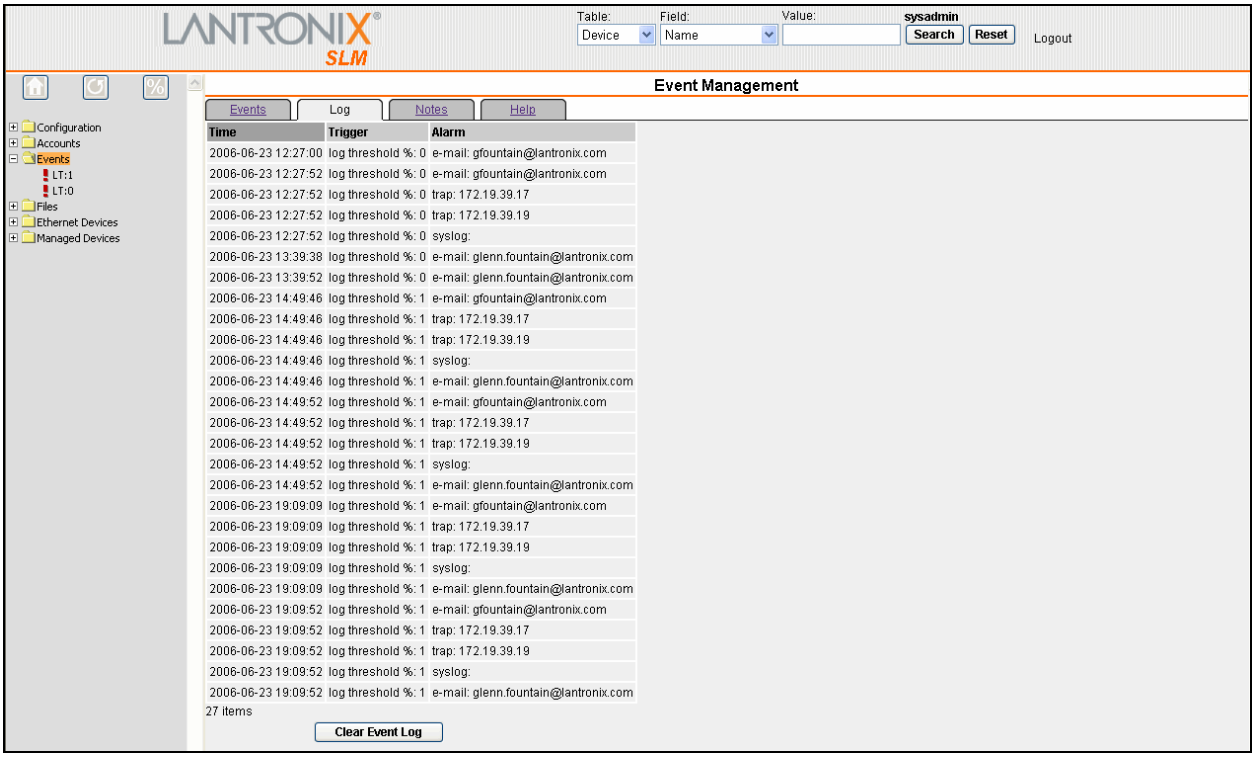
Viewing the Event Log

Administrators and authorized users view a list of all defined events.

To view all device events:

1. On the menu, click **Events** and then click the **Log** tab. The following page opens:

Figure 10-31. Event Management Page – Log Tab


LANTRONIX SLM
Table: Device
Field: Name
Value:
sysadmin
Search
Reset
Logout
Event Management
Events
Log
Notes
Help
Configuration
Accounts
Events
LT:1
LT:0
Files
Ethernet Devices
Managed Devices
Time Trigger Alarm
2006-06-23 12:27:00 log threshold %: 0 e-mail: gfountain@lantronix.com
2006-06-23 12:27:52 log threshold %: 0 e-mail: gfountain@lantronix.com
2006-06-23 12:27:52 log threshold %: 0 trap: 172.19.39.17
2006-06-23 12:27:52 log threshold %: 0 trap: 172.19.39.19
2006-06-23 12:27:52 log threshold %: 0 syslog:
2006-06-23 13:39:38 log threshold %: 0 e-mail: glenn.fountain@lantronix.com
2006-06-23 13:39:52 log threshold %: 0 e-mail: glenn.fountain@lantronix.com
2006-06-23 14:49:46 log threshold %: 1 e-mail: gfountain@lantronix.com
2006-06-23 14:49:46 log threshold %: 1 trap: 172.19.39.17
2006-06-23 14:49:46 log threshold %: 1 trap: 172.19.39.19
2006-06-23 14:49:46 log threshold %: 1 syslog:
2006-06-23 14:49:46 log threshold %: 1 e-mail: glenn.fountain@lantronix.com
2006-06-23 14:49:52 log threshold %: 1 e-mail: gfountain@lantronix.com
2006-06-23 14:49:52 log threshold %: 1 trap: 172.19.39.17
2006-06-23 14:49:52 log threshold %: 1 trap: 172.19.39.19
2006-06-23 14:49:52 log threshold %: 1 syslog:
2006-06-23 14:49:52 log threshold %: 1 e-mail: glenn.fountain@lantronix.com
2006-06-23 19:09:09 log threshold %: 1 e-mail: gfountain@lantronix.com
2006-06-23 19:09:09 log threshold %: 1 trap: 172.19.39.17
2006-06-23 19:09:09 log threshold %: 1 trap: 172.19.39.19
2006-06-23 19:09:09 log threshold %: 1 syslog:
2006-06-23 19:09:09 log threshold %: 1 e-mail: glenn.fountain@lantronix.com
2006-06-23 19:09:52 log threshold %: 1 e-mail: gfountain@lantronix.com
2006-06-23 19:09:52 log threshold %: 1 trap: 172.19.39.17
2006-06-23 19:09:52 log threshold %: 1 trap: 172.19.39.19
2006-06-23 19:09:52 log threshold %: 1 syslog:
2006-06-23 19:09:52 log threshold %: 1 e-mail: glenn.fountain@lantronix.com
27 items
Clear Event Log

Clearing the Event Log

Administrators can clear the event log.

To display current log information:

1. Click the **Refresh** button.

To clear the event log:

1. Click the **Clear Event Log** button. A message requesting confirmation displays.
2. In response to the confirmation message, click **OK**.

Files

Administrators can display and manage log, upgrade, configuration, session, and trap files of Ethernet devices.

Note: To retrieve files from the SLC, use the Manage SLC Group Actions tab.

File Types

You can view and store the following files in the SLM database. You can also import or export them by means of an NFS or CICS mount.

Firmware Upgrade

- **SLM FW Upgrade Files:** Files for upgrading the SLM's firmware.
- **SLC FW Upgrade Files:** Files for upgrading the SLC's firmware.
- **SLP FW Upgrade Files:** Files for upgrading the SLP's firmware.
- **Spider FW Upgrade Files:** Files for upgrading the Spider's firmware.
- **UDS FW Upgrade Files:** Files for upgrading the UDS's firmware.
- **WiBox FW Upgrade Files:** Files for upgrading the WiBox's firmware.

Note: You can obtain the most up-to-date firmware and release notes for the unit from the Lantronix web site (www.lantronix.com) or by using anonymous FTP (ftp.lantronix.com).

Configuration Files

- **SLM Configuration Files:** Contain all of the SLM's settings that have been saved to file. They can be backed up to a location that is not on the SLM.
- **SLC Configuration Files:** Contain all of the SLC's settings that have been saved to file. They can be backed up to a location that is not on the SLC.
- **SLC Sysconfig Files:** Contain status information about the SLC.

Log Files

- **SLM Syslog Files:** Contain information about all activity on the SLM (for example, login attempts, alarms, and diagnostics).
- **SLM Auditlog Files:** Every successful login, logout, and command on the command line interface and web is logged into a database table. The administrator reads this information from the CLI or web and creates an audit report for one or multiple users.
- **SLC/SLB Syslog Files:** Contain information about all activity on the SLC, for example, login attempts, alarms, and diagnostics.
- **SLC/SLB Auditlog Files:** Contain a log of all actions that have changed the configuration of the SLC.
- **SLC/SLB Portlog Files:** Contain a log of all actions and data on a specific port.

Session Files

- **SLC Port Active Files:** Contain session log files for currently active Secure Channel sessions to SLC device ports.

- **SLC Port Saved Files:** Contain archived session log files for Secure Channel sessions to SLC device ports. The files in the SLC Port Active Files directory move into the SLC Port Saved Files directory after the session ends.
- **SCS05/20 Port Session Files:** Contain session log files for SSH sessions to SCS05/20 device ports. There is no distinction between active and inactive sessions.
- **Device Session Files:** Contain session log files for Telnet/SSH/Secure Channel port sessions. There is no distinction between active and inactive sessions.

  *Note: Session log files can be accessed from the **Logs** tab of Ethernet devices and certain (SLC, SCS05/20) device ports, as well as through the appropriate folders under **Files→Session**.*

Trap Files

- **SLM Exported Trap Files:** Contains all or part of the trap log files as specified on the **Traps** tab of the All Ethernet Devices page.

File Format

The names of Device Session Files, SLC Port Saved Files, SCS05/20 Port Session Files, Device Session Files, and SLC Port Active Files have the following format:

<hostname>_<host_mac_address>-<device_port_number>=<username>=<connection_type>-<date_and_time>.log, where:

<hostname>	Up to the first 8 characters of the hostname of the Ethernet device. If the hostname is shorter than 8 characters, the hostname section is padded with ~ characters to reach this length.
<host_mac_address>	MAC Address of the Ethernet device. This is used by the SLM to correlate log files to their corresponding Ethernet devices.
<device_port_number>	Device port number connected to for this session. This field is set to 0 "00" for connections directly to the Ethernet device.
<username>	The SLM user ID that initiated this session.
<connection_type>	Session connection type: **tnt** for telnet, **ssh** for ssh, or **scc** for secure channel.
<date_and_time>	Date and time string in the format YYMMDD_HHMMSS

Note:** There is one more field after the date that enables **WHAT?

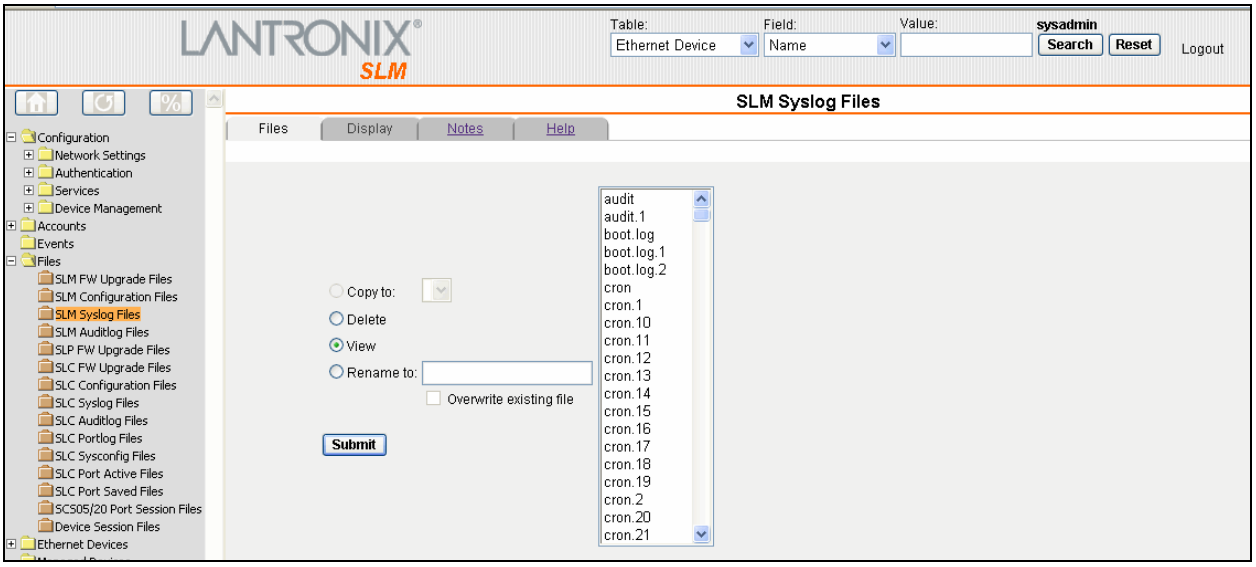
Viewing, Deleting, and Renaming Files

In this section, we show how to view, delete, and rename files. In our example, we use an SLM syslog file.

To view a file:

1. On the menu, click **Files** and then the file type you want to view. The following page opens:

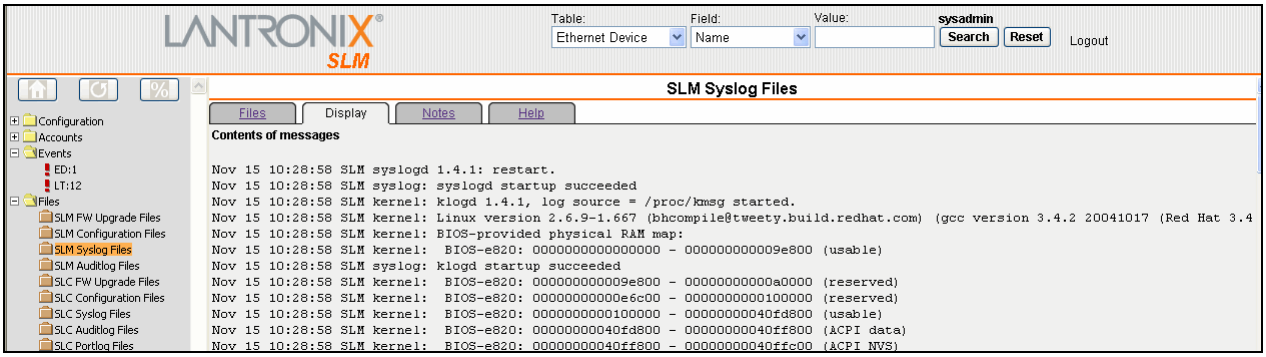
Figure 10-32. SLM Syslog Files Page – Files Tab



The available files (of the selected type) display in the list box.

2. Select **View** and then the file you want to view.
3. Click the **Submit** button. The **Display** tab opens and shows the contents of the selected file.

Figure 10-33. SLM Syslog Files Page – Display Tab


LANTRONIX
SLM
Table:
Ethernet Device
Field:
Name
Value:
sysadmin
Search
Reset
Logout
SLM Syslog Files
Files
Display
Notes
Help
Contents of messages
Nov 15 10:28:58 SLM syslogd 1.4.1: restart.
Nov 15 10:28:58 SLM syslog: syslogd startup succeeded
Nov 15 10:28:58 SLM kernel: klogd 1.4.1, log source = /proc/kmsg started.
Nov 15 10:28:58 SLM kernel: Linux version 2.6.9-1.667 (bhcompile@tweety.build.redhat.com) (gcc version 3.4.2 20041017 (Red Hat 3.4
Nov 15 10:28:58 SLM kernel: BIOS-provided physical RAM map:
Nov 15 10:28:58 SLM kernel: BIOS-e820: 0000000000000000 - 000000000009e800 (usable)
Nov 15 10:28:58 SLM syslog: klogd startup succeeded
Nov 15 10:28:58 SLM kernel: BIOS-e820: 000000000009e800 - 00000000000a0000 (reserved)
Nov 15 10:28:58 SLM kernel: BIOS-e820: 00000000000e6c00 - 0000000000100000 (reserved)
Nov 15 10:28:58 SLM kernel: BIOS-e820: 0000000000100000 - 00000000040fd800 (usable)
Nov 15 10:28:58 SLM kernel: BIOS-e820: 00000000040fd800 - 00000000040ff800 (ACPI data)
Nov 15 10:28:58 SLM kernel: BIOS-e820: 00000000040ff800 - 00000000040ffc00 (ACPI NVS)
Configuration
Accounts
Events
ED:1
LT:12
Files
SLM FW Upgrade Files
SLM Configuration Files
SLM Syslog Files
SLM Auditlog Files
SLC FW Upgrade Files
SLC Configuration Files
SLC Syslog Files
SLC Auditlog Files
SLC Portlog Files

To delete a file:

Note: *You cannot delete an active syslog file.*

1. On the menu, click **Files** and then the type of file. The files of that type in the database display in the list box.
2. Select **Delete** and then the file you want to delete. To select multiple files, use **Shift+click** or **Ctrl+click**.
3. Click the **Submit** button.
4. In response to the request for confirmation, click **OK**. The file is no longer in the list.
5. To see the status of the copy process if you are deleting multiple files at the same time, click the **Progress** button above the menu.

To rename a file:

Note: *You cannot rename an active syslog file.*

1. On the menu, click **Files** and then the type of file you want to rename. The files of that type display in the list box.
2. Select **Rename** and then the file you want to rename.
3. To rename a file to a name already in use in the directory, select the **Overwrite existing file** check box.

   Note: *If you try to rename a file to a name already in use in that directory, the rename will fail unless you select* ***Overwrite existing file*** *check box.*
4. Click the **Submit** button. A confirmation message displays.

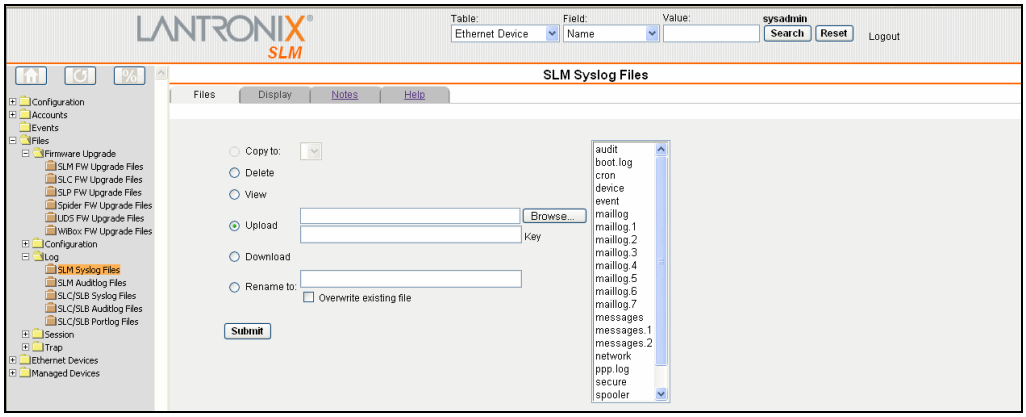
Exporting, Uploading, and Downloading Files

Administrators can export (copy), upload, and download files.

To open the Files page:

1. On the menu, click **Files** and then the file type you want to export. The following page opens:

Figure 10-34. Files Page



To export (copy) a file from the SLM to a mapped CIFS or NFS directory:

1. Select **Copy to**. The drop-down list box becomes active.

   Note: ***Copy To*** *is only active if CIFS or NFS has been configured or if USB flash memory is installed.*
2. From the drop-down list, select the location of the file (NFS or CIFS).
3. From the list box to the right, select the destination directory for the file (CIFS or NFS), and click the **Submit** button. To select multiple files, use **Shift+click** or **Ctrl+click**. A confirmation message displays.
4. To see the status of the copy process if you are copying multiple files at the same time, click the **Progress** button above the menu.

To upload a file from the client machine to the SLM:

1. On the menu, click **Files** and then the file type you want to upload. The following page displays:
2. Select **Upload**.
3. Click the **Browse** button and locate the file on your client machine to upload.
4. If this is an SLM FW Upgrade or SLC FW Upgrade (which also handles SLB), enter the md5sum value for this file in the **Key** field.
5. Click the **Submit** button. The file displays in the list box.

To download a file from the SLM and to the client machine:

1. On the menu, click **Files** and then the file type you want to download.
2. Select **Download**.
3. Select the file to download from the files list.
4. Click the **Submit** button. A confirmation message displays.
5. If necessary, when requested by your browser, select the destination directory for the file on your client machine.

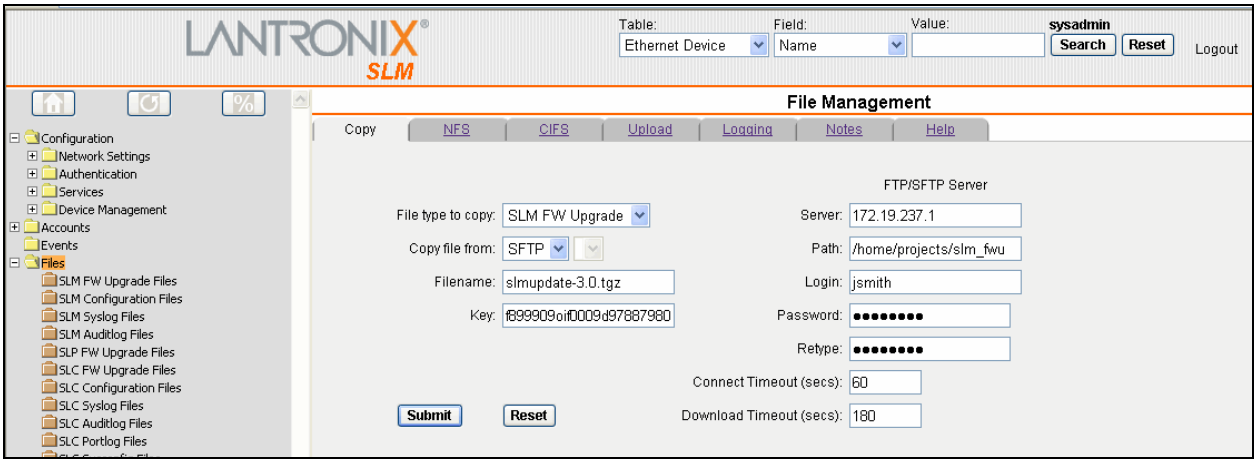
Copying Files

The administrator and other authorized users can download SLM and SLC firmware upgrade, configuration, and log files from an FTP/SFTP server.

To copy a file:

1. On the menu, click **Files**. The following page opens:

Figure 10-35. File Management Page – Copy Tab



2. Enter the following:

File type to copy	From the drop-down list, select the type file to copy. The default setting is **SLM FW Upgrade**.
Copy file from	Select the type of server from which to copy. The default setting is **SFTP**. ***Note:*** *If you set up NFS and CIFS, or if a USB flash memory is installed, then they display in this list.*

Filename	Name of the firmware upgrade or configuration file.
Key	A key for validating the firmware file. The key comes with the firmware file (32 hex characters).

3. Enter the following information about the destination server:

FTP/SFTP Server

Server	The IP address or host name of the server used for obtaining upgrades and saving or restoring configurations. May have up to 64 alphanumeric characters; may include hyphens and underscores.
Path	The default path on the server for obtaining firmware upgrade files and getting and putting configuration save files.
Login	The user ID for accessing the FTP or SFTP server. May be blank.
Password and **Retype**	The FTP or SFTP user password.
Connect Timeout (secs)	The number of seconds after which the connection attempt times out. Default is **60**.
Download Timeout (secs)	The number of seconds after which the download attempt times out. Default is **180**.

4. To save, click the **Submit** button.
5. To see the status of the copy process if you are copying multiple files at the same time, click the **Progress** button above the menu.

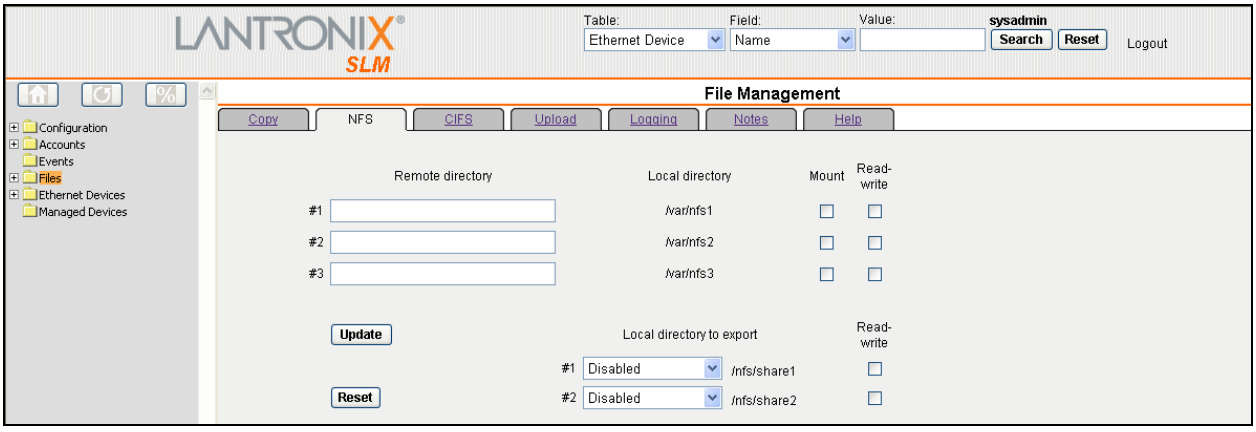
Setting up NFS

You can import files from or export files to a remote NFS server. The administrator defines the remote and local directories and read/write permissions.

To set up NFS:

1. On the menu, click **Files** and then the **NFS** tab. The following page opens:

Figure 10-36. File Management Page – NFS Tab



2. Enter the following information for importing a file:

Note: *The first three lines are for mounting remote NFS directories (the SLM functions as an NFS client). Once the directory is mounted, the SLM can import files from that share point.*

Remote directory	The remote NFS share directory in the format: **<nfs_server_hostname_or_ipaddr>:/<nfs_mount_point>** where **<nfs_mount_point>** is the path to the exported NFS directory on the remote NFS server.
Local directory	The local directory on the SLM on which to mount the remote directory. The SLM creates the local directory automatically.
Mount	Select the check box to enable the SLM to import the file by means of the NFS server. Disabled by default.
Read-write	If enabled, indicates that the user can read or write to the exported directory.

3. Enter the following information about exporting a file from the SLM:

   Note: *This information is for exporting NFS shares (the SLM functions as an NFS server). This allows remote NFS clients to mount these shares and then view/update the files in the exported directories*.

Local directory to export #1 and #2	From the drop-down list, select up to two directories to export. Disabled by default.
Read-write	If enabled, indicates that the user can read or write to the exported directory.

4. Click the **Update** button. When the update is complete, a confirmation message displays in the bottom part of the page.

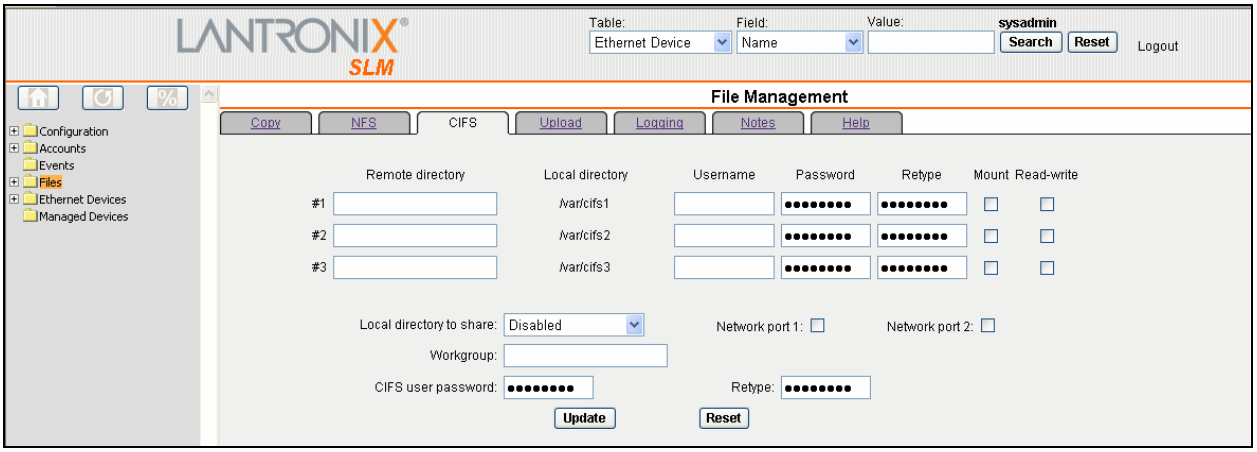
Setting up CIFS

Administrators can import files from or export files to a local or remote CIFS server. You define the remote and local directories, passwords, and read/write permissions.

To set up CIFS:

1. On the menu, click **Files** and then the **CIFS** tab. The following page opens:

Figure 10-37. File Management – CIFS Tab



2. Enter the following information for importing a file:

Note: *The first three entries are for mounting remote CIFS/Samba shares (the SLM acts as a CIFS client). The username and password are required to authenticate users on the remote CIFS server. The second section on this page is for the CIFS share that we can export (the SLM acts as a CIFS server).*

Remote directory	The remote directory to be imported, in the format: **//<server_name_or_ip>/<sharepoint>**.
Local directory	The local directory on the SLM on which to mount the remote directory. The SLM creates the local directory automatically.
Username	User name required to authenticate the user on the remote CIFS server.
Password and **Retype**	Password required to authenticate the user on the remote CIFS server.
Mount	Select the check box to enable the SLM to import the file from the CIFS server. Disabled by default.
Read-write	If enabled, indicates that the user can read and write to the imported directory. Disabled by default.

3. Enter the following information about exporting a file from the SLM.

   Note: *This information is for the CIFS share that we can export (the SLM acts as a CIFS server).*

Local directory to share	From the drop-down list, select the directory you want the SLM to export. Disabled is the default setting.
Network port 1 and **Network port 2**	Select the network ports from which you can see the share. Normal usage is to make the share visible in both network ports, but the boxes are unchecked by default.
Workgroup	The Windows workgroup to which the PC importing the CIFS share belongs. Can have up to 15 characters.
CIFS user password and **Retype**	Only one special username (**cifsuser**) can access the CIFS share. Enter the CIFS user password in both password fields. The default user password is **CIFSPASS**. ***Note:*** *More than one user can access the share at the same time with the **cifsuser** user name and password.*

4. Click the **Update** button. When the update is complete, a confirmation message displays in the bottom part of the page.

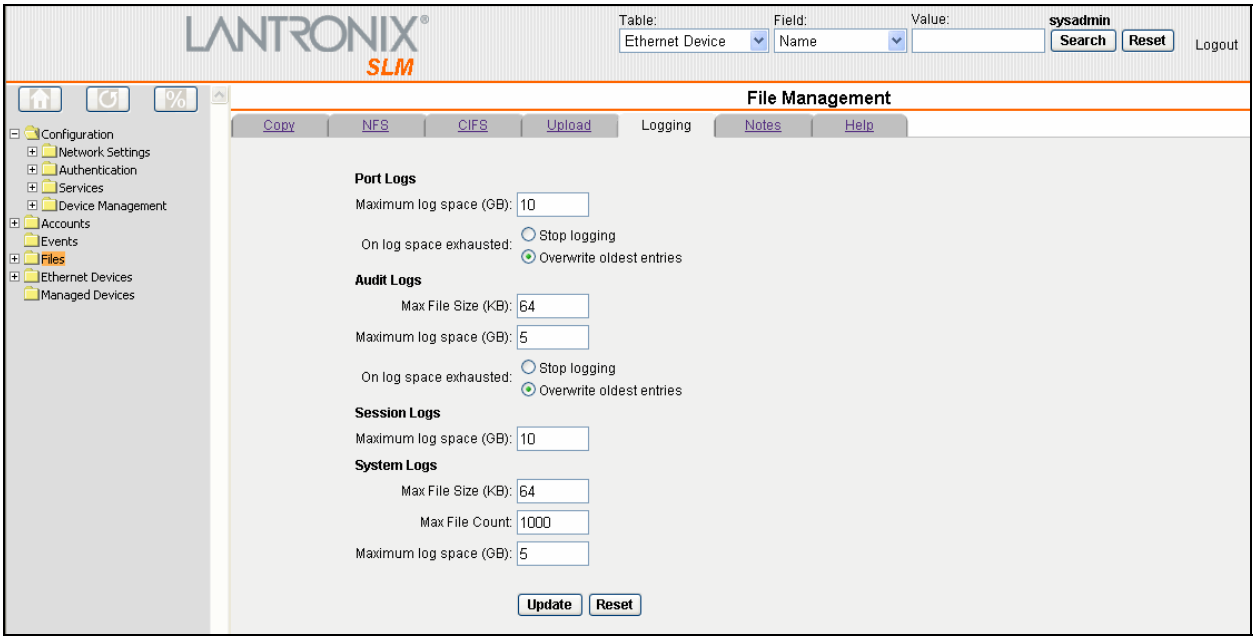
Setting up Log Properties

The administrator specifies the properties of log files.

To set up log properties:

1. On the menu, click **Files** and then the **Logging** tab. The following page opens.

Figure 10-38. File Management Page -- Logging Tab



2. Enter the following:

Port Logs

Maximum log space (30 GB available)	Maximum space used for all session log files in gigabytes. It is 30 GB for SLM-01 and 60 GB for SLM-02.
On log space exhausted	Select one of the following actions the SLM should take when all port log space has been used: **Stop logging:** When log space is exhausted, logging stops. **Overwrite oldest entries:** When port log space is exhausted, logging overwrites the oldest entries.

Audit Logs

Maximum File Size (KB)	Maximum size for each SLM audit log file in kilobytes. The default is **64**.
Maximum log space (GB)	Maximum space used for all SLM audit log files in gigabytes. The default is **5**.
On log space exhausted	Select one of the following actions the SLM should take when all audit log space has been used: **Stop logging:** When audit log space is exhausted, logging stops. **Overwrite oldest entries:** When audit log space is exhausted, logging overwrites the oldest entries.

Session Logs

Maximum log space (GB)	Maximum space used for all SLC session files in gigabytes. The default is **10**.

System Logs

Maximum File Size (KB)	Maximum size for each SLM system log file in kilobytes. The default is **64**.
Max File Count	Maximum number of system log files before the SLM starts to overwrite the old ones. The default is **1000**.
Maximum log space (GB)	Maximum space used for all SLM system log files in gigabytes. The default is **5**.

3. Click the **Update** button. When the update is complete, a confirmation message displays in the bottom part of the page.

Logging Commands

admin locallog

Syntax

```
admin locallog clear auditlog
admin locallog clear syslog
admin locallog clear traplog device <Device Name or IP Address>
admin locallog clear traplog group <group name>
group name: SLM, SLC, SLK, SLP, SCS, LTRX, or other
```

Description

Clears all of the entries in the auditlog, syslog, or traplog.

show auditlog

Syntax

`show auditlog`

Displays the audit log from the bottom.

`show auditlog tail`

Displays the audit log from the bottom (tail).

`show auditlog top`

Displays the audit log from the top.

Description

Displays the audit log. Default is `tail`.

show portlog

Syntax

`show portlog`
Lists all port log files.

`show portlog <parameters>`
Lists port log files as specified by parameters.

Parameters

[lastminutes <minutes>]

[date <MMDD>]

[date <MMDD-MMDD>]

Description

Lists portlog files.

Examples

`show portlog lastminutes 5`
Lists portlog files modifed in last 5 minutes.

`show portlog date 0205`
Lists portlog files last modified on 0205.

`show portlog date 0205-0209`
Lists portlog files last modified between 0205 and 0209.

show portlog file

Note: *Type* `show portlog` *to display index.*

Syntax

`show portlog file <index>`
Shows the port log from the top.

`show portlog file <index> tail`
Displays the port log from the bottom (tail).

`show portlog file <index> top`
Displays the port log from the top.

Description

Displays the contents of the portlog file by index. Default is `top`.

show portlog index

Syntax

Note: *Type* `show portlog` *to display index.*

`show portlog index <number>`
Displays part of portlog by index from the top.

Index is the number specified by `lastminutes` and date.
`show portlog index <number> <parameters>`

Parameters

`[top <number of lines>]`
Displays the part of portlog by index from the top.

`[tail <number of lines>]`
Displays the part of the portlog by index from the end.

`[lastminutes <minutes>]`

`[date <MMDD>]`

`[date <MMDD-MMDD>]`

Description

Displays the contents of the portlog file by index.

Note: *Index is the number specified by parameters* `lastminutes` *and* `date`*. If you specify* `0` *as number of lines, all lines display. If you specify both date and time, the SLM ignores the date option.*

Examples

`show portlog index 3`
Displays the specified portlog from top.

`show portlog index 3 top 10`
Displays the first 10 lines of specified portlog from top.

`show portlog index 3 tail 15`
Displays the last 15 lines of specified port log from tail.

`show portlog index 3 lastminutes 5`
Displays port log by the index '3'.
To get this index, type `show portlog lastminutes 5`.

`show portlog index 3 date 0205`
Displays port log by the index '3'.
To get this index, type `show portlog date 0205`.

`show portlog index 3 date 0205-0209`
Displays port log by the index '3'.
To get this index, type `show portlog date 0205-0209`.

`show portlog index 3 top 10 lastminutes 5`
Displays the first 10 lines of portlog by the index '3'.
To get this index, type `show portlog lastminutes 5`.

`show portlog index 3 tail 0 lastminutes 5`
Displays the portlog by the index '3' from tail.
To get this index, type `show portlog lastminutes 5`.

show portlog list

Syntax

`show portlog list`

`show portlog list <parameters>`

Parameters

`[lastminutes <minutes>]`

`[date <MMDD>]`

`[date <MMDD-MMDD>]`

Description

Lists portlog files in short form.

show sessionlog

Syntax

```
show sessionlog type <sessiontype> <parameters>

sessiontype: <slcportactive|slcportsaved|scsport|device>
```

Parameters

```
[lastminutes <minutes>]

[date <MMDD>]

[date <MMDD-MMDD>]
```

Description

Lists session log files.

Examples

`show sessionlog`
Lists device session log files.

`show sessionlog type slcportsaved lastminutes 5`
Lists archived SLC port session log files modified in last 5 minutes.

`show sessionlog date 0205`
Lists session log files last modified on 0205.

`show sessionlog type scsport index 3`
Displays the specified SCS05/20 port session log from the top.

`show sessionlog type device index 3 top 10`
Displays the first 10 lines of the specified device session log from the top.

`show sessionlog type device index 3 tail 15`
Displays the last 15 lines of specified device session log from the end.

`show sessionlog type device index 3 lastminutes 5`
Displays device session log by the index '3'.
To get this index, type `show portlog lastminutes 5`.

`show sessionlog type slcportsaved index 3 date 0205`
Displays archived SLC port sessionlog by the index '3'.
To get this index, type `show sessionlog type slcportsaved date 0205`.

`show sessionlog type device index 3 date 0205-0209`
Displays device session log by the index '3'.
To get this index, type `show sessionlog type device date 0205-0209`.

`show sessionlog type device index 3 top 10 lastminutes 5`
Displays the first 10 lines of device session log by the index '3'.
To get this index, type `show sessionlog type device lastminutes 5`.

show syslog

Syntax

`show syslog`

Shows the syslog information.

`show syslog tail`

Displays the syslog from the bottom (tail).

`show syslog top`

Displays the syslog from the top.

Description

Shows the syslog information. Default is `tail`.

show traplog index

Syntax

`show traplog [index <number>]`

Description

Displays all current trap log information. The index number displays detailed information about a selected trap log.

show traplog device

Note: *Type* `show traplog` *to display the index.*

Syntax

show traplog device <Device Name or IP address> [index <number>]

Description

Displays the current trap log information for an Ethernet device using name, IP address, or index number.

show traplog group

Note: *Type* `show traplog` *to display the index.*

Syntax

`show traplog group <Device Group Name> [index <number>]`

Group name: `SLM, SLC, SLK, SLP, SCS, LTRX`, or `other`

Description

Displays the current trap log information for an Ethernet device group by index number.

11: Using SLM on a Mobile Browser

SLM's WAP technology enables you to access the status of your SLM from your mobile phone. This chapter familiarizes you with how to do this. For more detailed information about the options, please see the other chapters in this User Guide.

Requirements

- To access SLM for mobile web browsers, your phone must meet the following minimum requirements:
- Your phone's web browser must be XHTML Mobile 1.0-compliant, which most mobile browsers are.
- If you want to access the SLM WAP site via SSL (https), your phone browser must support SSL. An example of such a browser is Opera Mini.
- Your phone's browser does not need to support cookies or JavaScript.
- Your wireless provider may charge you, Depending on your service plan, Check with your provider for more information about fees associated with accessing the Internet from your mobile phone.

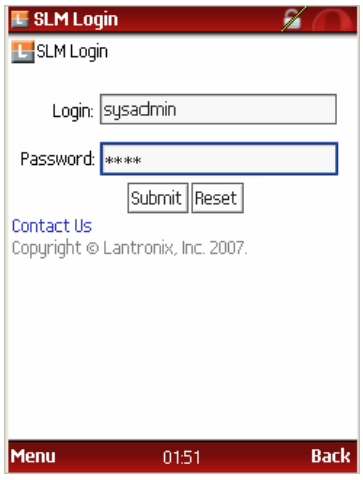
Using the SLM Mobile Browser

Logging in to the SLM

To log into the SLM:

1. Enter http://(SLM's IP address)/wap or https://(SLM IP address)/wap in your phone's web browser to log in to SLM.

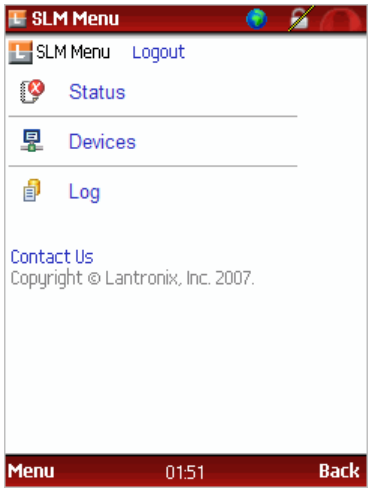
   The Login page displays.



2. Enter your SLM login name and password.

3. Move the cursor to the **Submit** button and select it.

   The SLM main menu (Home page) displays a list of options:



Using Links to Select Options

To select an option:

1. Click the link (blue). For example, click **Log** on the Home page to display a menu of logs.

Using the Keypad to Select Options

Note: *Shortcut keys only work with a true WAP browser (not browsers such as IE or FireFox).*

1. When a number precedes an option, tap the number on the keypad to open the link.

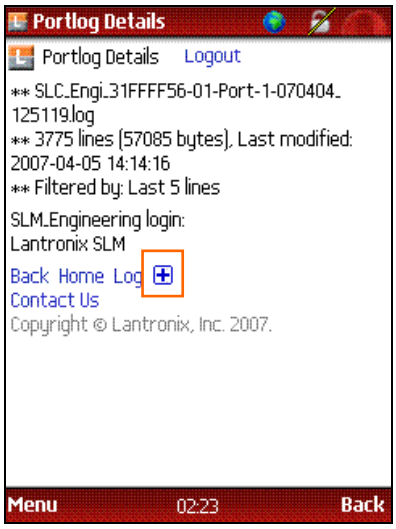
For example, to select **Managed Devices** in the example above, tap the **3** key.

Obtaining More Data

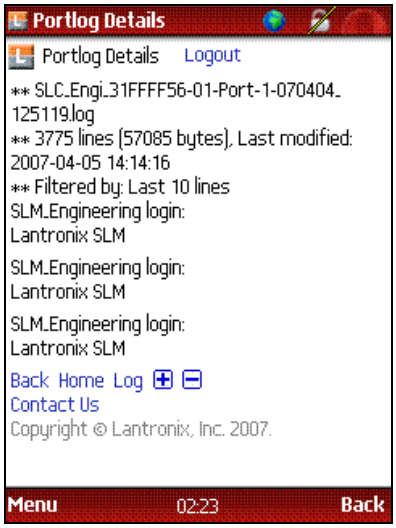
A **+** (plus) and/or a – (minus) button may display at the bottom of a page.

- If there is a **+**, select it or tap the ***** (star key) to advance to the next page of details.
- If there is **–** (minus), select it or tap the **#** (pound key) to return to the previous page.

For example, towards the bottom of the Portlog Details page, the **+** symbol displays.



If you select the **+**, further details display.



If you select the **–**, the previous page of details displays.

Logging Out

To log out of the SLM:

1. Select **Logout** (at the top right of each page).

Navigation Summary

To	Select on the browser page	Tap on the keypad
Return to the Home page	Home (bottom of page)	**0** (zero)
Select menu option	Link (blue)	When a number precedes an option, the number on the keypad.
See more details (if available)	**+**	* (star key)
Return to previous details	**–**	**#** (pound key)
Return to the previous page	Back (bottom of page)	Back or its equivalent on your phone
Return to a menu	Name of menu (if at bottom of page)	
Log out	Logout (top of any page)	

Main Menu

To use the SLM Menu (main menu):

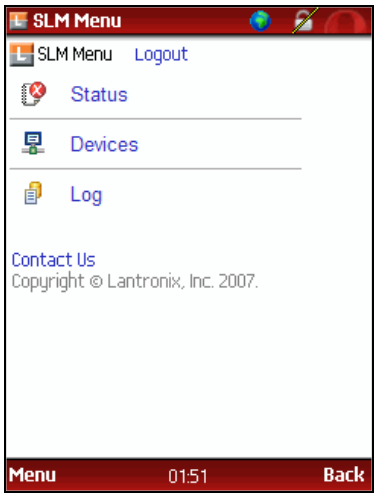
1. To use the main menu, select one of the following links:

   Status: Displays the status of the SLM.

   Devices: Displays information about Ethernet and Managed devices.

   Log: Displays audit, port, system, and trap logs.

.



The menu for the selected category opens

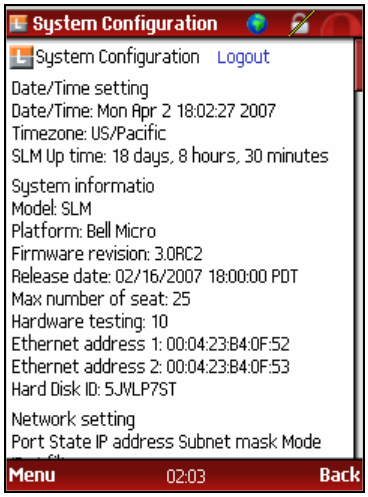
Status Menu

The SLM Status menu has three options: System Information, Connections, and Routes.

System Information

To view the status of the system:

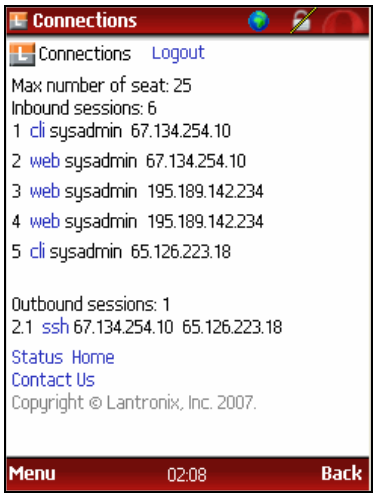
1. On the Status Menu, select **System Information** or tap the **1** key. The system configuration displays.



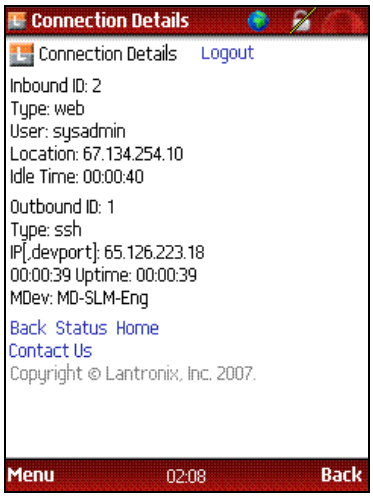
Connections

To view information about the SLM's connections:

1. On the Status Menu, select **Connections** or tap the **2** key. The Connections menu displays.



2. To view individual connections, click the blue link on the Connections menu or tap the key number displayed to the left of the option.



Route Information

To view SLM route information:

1. On the Status Menu, select **Routes**, or tap the **3** key.

Device Menu

The Device Menu provides access to Ethernet devices, unreachable Ethernet devices, and Managed Devices.

To view information about the devices the SLM is managing:

1. On the Main menu, select **Devices**. The Devices menu displays.

Ethernet Devices

To view information about an Ethernet device:

1. From the Devices menu, select **Ethernet Devices**.

The green icon to the right of a device indicates that the device is reachable; the red indicates that the device is unreachable.

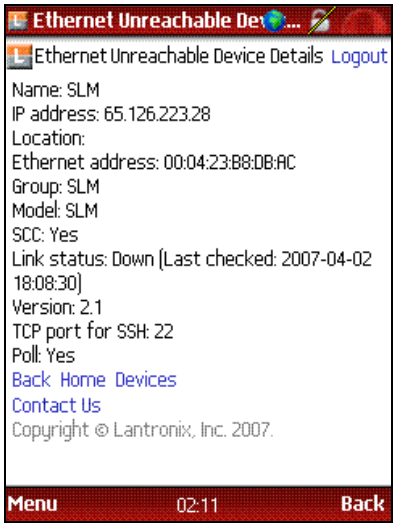
2. Select the unit you want to view. Details about the device display.

Ethernet Unreachable Devices

To view Ethernet devices to which the SLM has not been able to connect:

1. On the Devices menu, select **Ethernet Unreachable Devices**. The Ethernet Unreachable Devices page displays a list of unreachable devices.

2. To view device details, select the device.



Managed Devices

To obtain information about managed devices:

1. Select **Managed Devices** on the Devices menu. The Managed Devices page displays a list of managed devices.

2. Select a managed device to view its details.

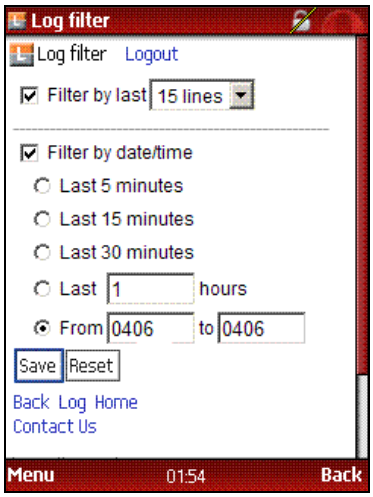
Log Menu

Filtering Logs

The Log filter page enables you to view logs matching specified criteria (number of lines and date/time). The settings are for the current session only. Once you save the filter, it applies for all log commands and is available as long as you are on the system (until logout or timeout).

To define a filter:

1. Click the **Filter** link at the bottom of the Log menu. The Log Filter page displays.



2. Select one or both of the following:

Filter by last	Select the check box and from the drop-down list, select the number of lines at the end of the log you want to see.
Filter by date/time	Select the check box and time period you want to see.

3. Select the **Save** button.

Example:

If you set **Filter by last** to 5 in log filter page and enable the filter, only the last 5 lines of a log file displays.

When you select **+**, it displays 10 (2X5), if available

When a user select **+** again, it displays 15 (3X5), if available

Minus works in the other direction.

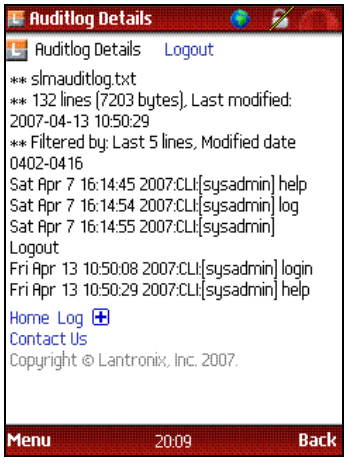
View Logs

To view audit, trap, system, or port logs:

1. Select **Log** on the Main menu. The SLM Log menu displays.

2. Select the type of log you want to see (e.g., tap **2** to see the SLM's audit logs).

3. Select the log to view details.


Auditlog Details
Auditlog Details Logout
** slmauditlog.txt
** 132 lines (7203 bytes), Last modified: 2007-04-13 10:50:29
** Filtered by: Last 5 lines, Modified date 0402-0416
Sat Apr 7 16:14:45 2007:CLI:[sysadmin] help
Sat Apr 7 16:14:54 2007:CLI:[sysadmin] log
Sat Apr 7 16:14:55 2007:CLI:[sysadmin] Logout
Fri Apr 13 10:50:08 2007:CLI:[sysadmin] login
Fri Apr 13 10:50:29 2007:CLI:[sysadmin] help
Home Log
Contact Us
Copyright © Lantronix, Inc. 2007.
Menu 20:09 Back

4. Select the **+** button to see more details.

Auditlog Details
Auditlog Details Logout
** slmauditlog.txt
** 132 lines (7203 bytes), Last modified: 2007-04-13 10:50:29
** Filtered by: Last 5 lines, Modified date 0402-0416
Sat Apr 7 16:14:45 2007:CLI:[sysadmin] help
Sat Apr 7 16:14:54 2007:CLI:[sysadmin] log
Sat Apr 7 16:14:55 2007:CLI:[sysadmin] Logout
Fri Apr 13 10:50:08 2007:CLI:[sysadmin] login
Fri Apr 13 10:50:29 2007:CLI:[sysadmin] help
Home Log
Contact Us
Copyright © Lantronix, Inc. 2007.
Menu
20:09
Back

5. Select the + to scroll to see more lines of details.

Note: *You can set the number of lines you see at a time on the Log filter page.*

A: Command Reference

After an introduction to using commands, this chapter lists and describes all of the commands available on the SLM command line interface accessed through SSH, secure channel (SLC only), Telnet, or a serial connection. The commands are in alphabetical order by category.

Introduction to Commands

Command Syntax

Commands have the following format:

`<action> <category> <parameter(s)>`

where

`<action>` is set, show, connect, diag, admin, or logout.

`<category>` is a group of related parameters you want to configure or view. Examples are devicegroup, account, and network.

`<parameter(s)>` is one or more name-value pairs in one of the following formats:

`<parameter name> <aa|bb>`	Specify one of the values (aa or bb) separated by a vertical line (|). The values are all lowercase and must be entered exactly as shown. Bold indicates a default value.
`<parameter name> <Value>`	Specify an appropriate value, for example, a device group name. This User Guide shows parameter values in mixed case to indicate they are case sensitive. For example, if you saved a device group name in mixed case, you must enter it in mixed case; if you saved it in lowercase, you must enter it in lowercase.
Square brackets [ ]	Indicate optional parameters.

Figure 11-1. Actions and Category Options

Action	Category
set	network | service | ipfilter | account | accountgroup | auth | | nis | ldap | radius | kerberos | tacacs+ | securid |ethernetdevice | manageddevice | datetime |cli | menu | sshkey | history | modem | dialaccount
show	network | service | ipfilter | iptables |account| accountgroup | auth | nis | ldap | radius | kerberos | tacacs+ | securid | device | port | ethernetdevice | manageddevice | auditlog |syslog| portlog | traplog | eventlog | sessionlog |datetime | cli | menu | sshkey | history | connection | progress | sysconfig | modem | dialaccount | routing
connect	device | index | ssh | telnet | terminate
diag	ping | ping6 | nettrace | arp | traceroute | netstat
admin	autodetect | locallog | version | productkey | option | config | quicksetup | securechannel | signature | banner | reboot | shutdown | showbootbank | switchbank | copybank
logout	Terminates CLI session.

Command Help

For general command help, type: **`help`**

For more information about a specific command, type **`help`** followed by the command, for example:

```
help set network
```

OR

type **`?`** after the command:

```
set network ?
```

Tips

- Type enough characters to identify the action, category, or parameter name uniquely. For parameter values, type the entire value. For example,

  ```
  set network port 1 state static ipaddr 122.3.10.1 mask 255.255.0.0
  ```

  can be shortened to:

  ```
  se net po 1 st static ip 122.3.10.1 ma 255.255.0.0
  ```

- Use the **Tab** key to automatically complete action, category, or parameter names. Type a partial name and press **Tab** to complete the name if only one is possible, or to display the possible names if more than one is possible.
- Should you make a mistake while typing, backspace by pressing the **Backspace** key or the **Delete** key, depending on how you accessed the interface. Both keys work if you use VT100 emulation in your terminal access program when connecting to the console port. Use the **left** and **right arrow** keys to move within a command.

- Use the **up** and **down arrows** to scroll through previously entered commands. If desired, select one and edit it. You can scroll through up to 100 previous commands entered in the session.
- When the number of lines displayed by a command exceeds the size of the window (the default is 20), the "`Type more to see the next page`" `message displays`. To display the next page, type **`more`** and press **Enter**. You can override the number of lines (or disable the feature altogether) with the `set cli` command.
- To clear an IP address, type **`0.0.0.0`**.

Authentication Commands

set auth

Syntax

```
set auth <one or more parameters>
```

Parameters

```
local <1-7>
nis <1-7>
ldap <1-7>
radius <1-7>kerberos <1-7>
tacacs+ <1-7>
securid <1-7>
authusenextmethod <enable|disable>
limitsysadmin <enable|disable>
```

Description

Sets ordering of authentication methods and how authentication methods are used.

Authentication can occur using all methods, in the order of their precedence, until a successful authentication is obtained, or using only the first authentication method that responds (in the event that a server is down).

Note: *If SecurID is used, no other parameters can be used.*

Any methods omitted from the `set auth` command will be disabled if at least one method is selected

set ldap

Syntax

```
set ldap <one or more parameters>
```

Parameters

```
state <enable|disable>
server <IP Address or Name>
 port <TCP Port>
 base <LDAP Base>
```

```
bindname <Bind Name>
bindpassword <Bind Password>
adsupport <enable|disable>
encrypt <enable|disable>
```

Description

Configures the SLM to use LDAP to authenticate users who log in to the SLM via SSH, Telnet, the web, or the console port.

set nis

Syntax

```
set nis <one or more parameters>
```

Parameters

```
<enable|disable>
domain <NIS Domain Name>
broadcast <enable|disable>
master <IP Address or Name>
slave1 <IP Address or Name>
slave2 <IP Address or Name>
slave3 <IP Address or Name>
slave4 <IP Address or Name>
slave5 <IP Address or Name>
```

Description

Configures the SLM to use NIS to authenticate users who log in to the SLM via SSH, Telnet, the web, or the console port.

set radius

Syntax

```
set radius <one or more parameters>
state <enable|disable>
timeout <1-30 seconds>
server1 <IP Address or Name>
port1 <TCP Port>
secret1 <Secret>
server2 <IP Address or Name>
port2 <TCP Port>
secret2 <Secret>
```

Description

Configures the SLM to use RADIUS to authenticate users who login to the SLM via SSH, Telnet, the web, or the console port.

set sshkey delete

Syntax

```
set sshkey delete keyuser <SSH Key User> keyhost <SSH Key Host>
```

Description

Deletes an imported SSH key.

set sshkey import

Syntax

```
set sshkey import <copypaste>
```

Note: RSA keys must be 1024 bits

Description

Imports an SSH key.

show auth

Syntax

```
show auth
```

Description

Displays authentication methods in use.

show ldap

Syntax

```
show ldap
```

Description

Displays all LDAP information.

show nis

Syntax

```
show nis
```

Description

Displays all NIS information.

show radius

Syntax

show radius

Description

Displays all RADIUS information.

show sshkey import

Syntax

```
show sshkey import <one or more parameters>
```

Parameters

[keyuser <SSH Key User>]

[keyhost <SSH Key IP Address or Name>]

[viewkey <enable|disable>]

Description

Displays imported SSH keys.

Account Commands

Use the following commands to configure local accounts (including **sysadmin**) to authenticate users who login to the SLM by means of SSH, Telnet, the web, or the console port.

set account add

Syntax

set account add <User Name> group <Group Name|admin>> <parameters>

Parameters

[email <Email Address>]

[auth <local|remote|localremote|disable>]

[allowdialback <enable|disable>]

[dialbacknumber <dial-back number>]

[allowpwchange <enable|disable>]

[pwneverexpires <enable|disable>]

[changepwnextlogin <enable|disable>]

Description

Creates a new user account.

set account delete

Syntax

set account delete <User Name>

Description

Deletes a user account.

set account edit

Syntax

set account edit <User Name> group <Group Name|admin> <parameters>

Parameters

[email <Email Address|CLEAR>]

Email CLEAR removes the current email.

[auth <local|remote|localremote|disable>

[allowdialback <enable|disable>]

```
[dialbacknumber <dial-back number|CLEAR>]
[allowpwchange <enable|disable>]
[pwneverexpires <enable|disable>]
[changepwnextlogin <enable|disable>]
```

Description

Modifies a user account.

set account password

Syntax

```
set account password <User Name>
```

Note: *Administrators with permission to change passwords must enter the username. Other users may not enter a username (they are changing their own password).*

Description

Configures a user account's password for the SLM.

show account

Syntax

```
show account <User Name>
show account user <User Name>
```

Description

Displays account information by user name.

show account all

Syntax

```
show account all
show account
```

Description

Displays all account names and information.

show account index

Note: *Type* `show account all` *to display the index.*

Syntax

```
show account index <number>
```

Description

Displays accounts by index number.

show account search

Syntax

Note: *All searches are case insensitive.*

```
show account search name <name>
show account search email <email address>
```

Examples

```
show account search name sys
```

Description

Searches for accounts by name or email address.

Account Group Commands

set accountgroup add

Syntax

```
set accountgroup add <Group Name> type <ethernet|managed|menu>
<parameters>
```

Parameters

```
[menu <Menu Name>]
```

Description

Creates a local account group. Group type is Administrators, Ethernet, Managed, or Menu User.

set accountgroup edit

Syntax

```
set accountgroup edit <Group Name> <one or more parameters>
```

Parameters

```
[name <new name>]
[menu <Menu Name|CLEAR>]
```

Description

Modifies an account group. Group type is Administrators, Ethernet User, Managed User, or Menu User. `CLEAR` removes the current menu assignment.

show accountgroup

Syntax

```
show accountgroup <Group Name>
show accountgroup name <Group Name>
```

Description

Displays account group information.

show accountgroup all

Syntax

```
show accountgroup all
show accountgroup
```

Description

Displays information about all account groups.

show accountgroup index

Note: *Type* `show accountgroup all` *to display the index.*

Syntax

```
show accountgroup index <number>
```

Description

Displays account groups by index number.

Administrative Commands

admin autodetect filter

Syntax

```
admin autodetect filter delete
```

Deletes one of the current auto-detect search filters. The command displays an index of current filters. Type the index number of the filter you want to delete and press **Enter**.

```
admin autodetect filter ltrx <IP subnet>
```

Sets Lantronix discovery protocol search filters.

```
admin autodetect filter scs <IP range> [timeout <number of
milliseconds>]
```

Sets SCS discovery protocol search filters.

Example

```
IP range: 192.168.0.1-192.168.0.155
timeout : 100ms (default)
```

```
admin autodetect filter snmp <IP range> [community <name>]
```

Sets SNMP protocol search filters.

Example

```
IP range: 192.168.0.1-192.168.0.155
name: public (default)
```

```
admin autodetect filter show
```

Displays the current auto-detect search filters.

Description

Configures or displays the protocol and filters.

admin autodetect start

Syntax

```
admin autodetect start
```

Description

Starts the SLM auto-detect device process, using the protocol and filters configured.

admin banner

Syntax

```
admin banner welcome <Banner Text>
admin banner login <Banner Text>
admin banner logout <Banner Text>
```

Description

Configures the banner displayed before login (welcome), after login, or after logout. To insert line feeds in the banner, use the '\\n' character sequence.

admin banner show

Syntax

```
admin banner show
```

Description

Displays the banner configuration.

admin copybank

Syntax

```
admin copybank
```

Description

Copies the SLM firmware running in the current bank to the other bank.

admin config

Syntax

```
admin config factorydefaults
```

Description

Restores the SLM configuration and device database settings to factory defaults.

admin config rebuilddatabase

Syntax

```
admin config rebuilddatabase
```

Description

Removes and rebuilds the SLM configuration and database from scratch, in case of database corruption that cannot be fixed by the factory default.

admin locallog

Syntax

```
admin locallog clear auditlog
admin locallog clear syslog
```

```
admin locallog clear traplog device <Device Name or IP Address>
admin locallog clear traplog group <group name>
group name: SLM, SLC, SLK, SLP, SCS, BOB, SPDR, WiBox, LTRX, or
other
```

Description

Clears all of the entries in the auditlog or syslog or traplog.

admin option

Syntax

```
admin option <Option Name> value <Option Value>
```

Description

Adds license options.

admin quicksetup

Syntax

```
admin quicksetup
```

Description

Displays the quick setup script on the CLI; only the sysadmin account can use this command.

admin reboot

Syntax

```
admin reboot
```

Description

Terminates all connections and reboots the SLM.

admin securechannel regenkey

Syntax

```
admin securechannel regenkey
```

Description

Regenerates the secure channel key.

Note: *With this command, you lose access to established secure channels; therefore, the SLM first requests confirmation that you want to regenerate the secure channel key.*

admin showbootbank

Syntax

admin showbootbank

Description

Displays the SLM boot bank.

admin shutdown

Syntax

```
admin shutdown
```

Description

Terminates all connections, shuts down the SLM, and turns off the power.

admin switch bank

Syntax

```
admin swithchbank bank [1|2]
```

Description

Switches the SLM to the next boot bank.

admin signature restore

Syntax

```
admin signature restore
```

Description

Restores signature information to the system.

admin signature show

Syntax

```
admin signature show
```

Description

Displays signature information.

admin version

Syntax

```
admin version
```

Description

Displays current application version information.

show progress

Syntax

```
show progress
```

Description

Shows the progress of background tasks.

show sysconfig

Syntax

```
show sysconfig [email <Email Address>]
```

Description

Displays a report of configurable parameters. The output can be emailed.

All Devices Commands

show device

Note: Entries are not case sensitive.

Syntax

```
show device <device name>
```

Description

Searches for and displays Ethernet or managed devices by device name. For example, if you specify `name slc`, the SLM searches for all Ethernet and managed devices whose name starts with `slc`.

show device all

Syntax

```
show device all
```

```
show device
```

Description

Displays all Ethernet and managed devices.

show device index

Note: Type `show device all` to display the index.

Syntax

```
show device index <number>
```

Description

Displays Ethernet or managed devices by index.

Auto-Detect Commands

admin autodetect filter delete

Syntax

```
admin autodetect filter delete
```

The command displays an index of current filters. Type the index number of the filter you want to delete and press **Enter**.

Description

Deletes one of the current auto-detect search filters.

admin autodetect filter ltrx

Syntax

```
admin autodetect filter ltrx <IP range> [timeout <number of
milliseconds>]
```

Example

```
IP range: 192.168.0.1-192.168.0.155 timeout 1500
timeout: default is 1000 ms; range is 1000-60000 ms
```

Description

Sets Lantronix discovery protocol search filters. The ending IP address is optional.

admin autodetect filter scs

Syntax

```
admin autodetect filter scs <IP range> [timeout <number of
milliseconds>]
```

Example

```
IP range: 192.168.0.1-192.168.0.155
timeout: default is 100 msec; range is 100-60000 msec
```

Description

Sets SCS discovery protocol search filters.

admin autodetect filter show

Displays the current auto-detect search filters.

Syntax

```
admin autodetect filter show
```

Description

Displays the current auto-detect search filters.

admin autodetect filter snmp

Syntax

```
admin autodetect filter snmp <IP range> [community <name>]
[timeout <number of milliseconds>]
```

Example

```
IP range: 92.168.0.1-192.168.0.155
name: public (default)
timeout:default is 100 msec; range is 100-60000 msec
```

Description

Sets SNMP protocol search filters.

admin autodetect start

Syntax

```
admin autodetect start <one or more parameters>
```

Parameters

`[securechannel <default|password>]`

`[option <ltrxonly|delnonltrx>}`
`ltrxonly` detects only Lantronix devices
`delnonltrx` detects only Lantronix devices and removes existing non-Lantronix devices.

Examples

```
admin autodetect start securechannel default
```

Attempts secure channel using the default password

`admin autodetect start securechannel mypass option delnonltrx`
Attempts secure channel using password `mypass`. Detects only Lantronix devices and removes existing non-Lantronix devices.

Description

Starts the SLM auto-detect device process, using the protocol and filters configured.

show progress

Syntax

`show progress`

Description

Shows the progress of background tasks.

CLI Commands

The following commands relate to the CLI itself.

set cli terminallines

Syntax

`set cli terminallines <disable|1-1000>`

Description

Sets the number of lines that display in a page for the auditlog, syslog, portlog, traplog, and device list. Default is **20**.

set history clear

Syntax

`set history clear`

Description

Clears the CLI command history.

show cli

Syntax

`show cli`

Description

Displays the terminal lines settings.

show history

Syntax

```
show history
```

Description

Displays the 100 most recent CLI commands.

Connection Commands

Administrators, Ethernet Users and Menu Only Users

connect device

Syntax

```
connect device <Device Name or IP Address> <one or more parameters>
```

Parameters

```
[<secure|ssh|telnet|serial|modem|modemssh|modemtelnet>][port <port>]
```

Specify `secure` to connect through a secure channel. Secure channel is the default method of connection for SLC, SLC ports, and SLM, and SSH is the default for other devices.

`Port` is the number of a physical port on the SLC.

Example

SLC48 has ports 1 to 48.

Modem connection is available for managed devices only.

With the `modemssh` option, the SLM dials out to the managed device in PPP, and then connects it via SSH.

With `modemtelnet` option, the SLM dials out to the managed device in PPP, and then connects it via Telnet.

Examples

```
connect device slc-waimea
connect device slc-waimea-port-1
connect device slc-waimea ssh
connect device slc-waimea port 4
connect device slc-waimea modemssh
```

Description

Connects to an Ethernet device, managed device, or device port.

connect index <number>

Note: *Type* `show device all` *to display the index.*

Syntax

```
connect index <number>
<secure|ssh|telnet|serial|modem|modemssh|modemtelnet>]
```

Description

Connects a device by index number.

connect ssh

Syntax

```
connect ssh <IP Address> [tcpport <TCP Port>] [<SSH flags>]
```

Parameters

`<SSH flags>` is one or more of:

```
user <Login Name>
version <1|2>
escape <Character>
```

The `TCP PORT` parameter is the TCP port number; the default is **22**.

Description

Connect to any machine/device using standard SSH V1 or V2 protocol.

connect telnet

Syntax

```
connect telnet <IP Address> [tcpport <TCP Port>] [user <Login
Name>]
```

`tcpport` is the TCP port number; the default is **23**.

Description

Connects to a device by means of standard Telnet.

show connection list

Syntax

```
show connection list
```

Description

Displays the active user connections in short form.

Managed Device Users

connect device

Syntax

connect device <Device Name>
[<secure|ssh|telnet|serial|modem|modemssh|modemtelnet>][port <port>]

Specify `secure` to connect through a secure channel. Secure channel is the default method of connection for SLC, SLC ports, and SLM, and SSH is the default for other devices.

Port is the number of a physical port on the SLC.

Example

SLC48 has ports 1 to 48.

Modem connection is available for managed devices only.

With the `modemssh` option, the SLM dials out to the managed device in PPP, and then connects it via SSH.

With `modemtelnet` option, the SLM dials out to the managed device in PPP, and then connects it via Telnet.

Examples

```
connect device slc-waimea
connect device slc-waimea-port-1
connect device slc-waimea ssh
connect device slc-waimea port 4
connect device slc-waimea modemssh
```

Description

Connects to a managed device through a secure channel.

connect index

Note: *Type* `show managedevice all` *to display the index.*

Syntax

```
connect index <number>
<secure|ssh|telnet|serial|modem|modemssh|modemtelnet>
```

Description

Connects to a device by index number.

Date and Time Commands

set datetime

Syntax

```
set datetime <one parameter>
```

Parameters

```
date <MMDDYYhhmm[ss]>
timezone <Time Zone>
```

Description

Sets the local date, time, and time zone (one parameter at a time).

Note: *If you type an invalid time zone, the system guides you through the process of selecting a time zone.*

show datetime

Syntax

```
show datetime
```

Description

Displays the local date, time, and time zone.

Diagnostic Commands

diag arp

Syntax

```
diag arp
```

Description

Displays the ARP table for mapping IP addresses to hardware addresses.

diag netstat

Syntax

```
diag netstat [<tcp|udp|all>] [statistics]
```

Description

Displays output IP routing table, and optionally, network connections and statistics.

diag nettrace

Syntax

`diag nettrace <one or more parameters>`

Parameters

```
ethport <1|2>]
protocol <tcp|udp|icmp>]
host <IP Address or Name>]
```

numpackets <number of packets>] [snaplen <capture bytes>]

verbose <0|**1**|2|3>]

Example

diag nettrace protocol udp verbose 2

Description

Displays all network traffic, applying optional filters.

diag ping

Syntax

diag ping <IP Address or Name> <one or more parameters>

Parameters

count <Number of Times to Ping>
Default is **5**.

packetsize <Size in Bytes>
Default is **64**.

Description

Verifies that the SLM can reach a host over the network.

diag ping6

Syntax

diag ping6 <IP Address or Name> <one or more parameters>

Parameters

interface <interface name>

count <Number of Times to Ping>
Default is **5**.

packetsize <Size in Bytes>
Default is **64**.

Examples

diag ping6 fe80::214:85ff:fec0:928e interface eth1

Description

Verifies that the SLM can reach a host over the network.

diag traceroute

Syntax

diag traceroute <IP Address **or** Name>

Description

Displays the route that packets take to get to a network host.

Dial Account Commands

set dialaccount add

Syntax

```
set dialaccount add <Dial Account Name> <parameters>
```

Parameters

modemmode <**text**|ppp>

Note: If you select `text`, all other parameters except `timeout` are ignored.

localipaddr <**negotiate**|IP Address>

remoteipaddr <**negotiate**|IP Address>

auth <**pap**|chap>

username <User Name>

password <Password>

nat <enable|**disable**>

timeout <disable|1-30 minutes>
Default is **20.**

Description

Creates a new dial account.

set dialaccount delete

Syntax

```
set dialaccount delete <Dial Account Name>
```

Description

Delete a dial account.

set dialaccount edit

Syntax

```
set dialaccount edit <Dial Account Name> <parameters>
```

Parameters

modemmode <text|ppp>

localipaddr <negotiate|IP Address>

remoteipaddr <negotiate|IP Address>

auth <pap|chap>

username <User Name>

password <Password>

nat <enable|disable>

forcedialback <disable|enable> (applies only to text mode)

dialbacknumber <dial-back number|CLEAR> (applies only to text mode)
CLEAR removes the dial-back number.

userprofile <disable|enable> (apply only text mode)

Uses local user-defined dial-back configuration.

```
timeout <disable|1-30 minutes>
```

Description

Modifies a dial account's settings.

set manageddevice config

Syntax

```
set manageddevice config <Device Name> [dialout <Dial Account
Name|enable|disable> modem <Modem Name> phonenumber <phonenumber>]
application <ssh|telnet|http|none>]
```

Description

Configures modem and dial account settings for a managed device.

set manageddevice index

Note: *Type* `show manageddevice all` *to display index.*

Syntax

```
set manageddevice index <number> [dialout <Dial Account
Name|enable|disable> modem <Modem Name> phonenumber <phonenumber>]
application ssh|telnet|http|none>]
```

Description

`Finds managed device by index and modifies dial account settings.`
To set modem parameters, you must specify a dial-out option.

set modem edit

Syntax

```
set modem edit <Modem Name> dialin <Dial Account
Name|CLEAR|disable|enable>
```

Description

Modifies a dial-in account name.

show dialaccount

Note: *Type* `show dialaccount` *to display index.*

Syntax

```
show dialaccount <parameters>
```

Parameters

```
[name <Dial Account Name>]
```

```
[index <number>]
```

Examples

```
show dialaccount
```

```
show dialaccount name ppp-pap
```

```
show dialaccount index 2
```

Description

Displays dial account settings.

show dialaccount mapping

Syntax

```
show dialaccount mapping
```

Description

Shows dial account used by dial-in and dial-out.

Ethernet Device Commands

set ethernetdevice config

Syntax

```
set ethernetdevice config <Device Name or IP Address> <one or
more parameters>
```

Parameters

```
[delete]

[dialout <Dial Account Name|enable|disable> phonenumber <phone
number>]

[disconnect modem]

[name <Device Name>]

[ipaddr <IP Address>]

[location <Location>]

[login <Loginname>]

[model <Model>]

[sshport <TCP Port for SSH>]

[version <Version>]
```

Description

Finds Ethernet devices by device name or IP address and modifies device parameters.

set ethernetdevice delete

Syntax

```
set ethernetdevice delete <Device Name or IP Address>
```

Finds Ethernet device using device name or IP address and deletes the device.

```
set ethernetdevice delete <Device Name or IP Address> portnumber
<port number or port number range>
```

`port number range`, for example, 1-4

Finds a port by Ethernet device name or IP address with the port number and deletes the port.

Examples

```
set eth delete slc-waimea

set eth delete slc-waimea port 5

set eth delete slc-waimea port 1-5

set eth conf slc-waimea delete
```

Description

Finds Ethernet device or Ethernet device port and deletes it.

set ethernetdevice port

Syntax

```
set ethernetdevice port <Device Name or IP Address> portnumber
<port number or list> <one or more parameters>
```

Parameters

```
[name <New Port Name>]
```

```
[state <on|off|cyclepower>]
```
(available for SLP only)
Powers Ethernet device port on or off.

Note: *Only SLP outlet action supports a port list.*

Examples

To power up SLP outlet 2:

```
set eth port slp-sunset po 2 state on
```

To power up SLP outlet port list 1-3,6,8-14

```
set eth port slp-sunset po 1-3,6,8-14 state on
```

Description

Finds a port by device name or IP address with the port number and modifies port parameters.

set ethernetdevice sync

Syntax

```
set ethernetdevice sync <Device Name or IP Address> action
<read|write>
```

Description

Finds an Ethernet device-by-device name or IP address and synchronizes device information.

show device

Note: *Entries are not case sensitive.*

Syntax

```
show device <device name>
```

Description

Searches for and displays Ethernet or managed devices by device name.

show device all

Syntax

```
show device all
```

```
show device
```

Description

Displays all Ethernet and managed devices.

show ethernetdevice all

Syntax

```
show ethernetdevice all
```

Description

Displays all Ethernet device information.

show ethernetdevice config

Syntax

```
show ethernetdevice config <Device Name or IP Address>
```

Description

Finds an Ethernet device-by-device name or IP address and displays device information.

show ethernetdevice firmware

Syntax

```
show ethernetdevice firmware
```

Description

Displays firmware versions of all Ethernet devices managed by the SLM.

show ethernetdevice group

Syntax

```
show ethernetdevice group <Group Name> [firmware]
```

`group name`: SLM, SLC, SLK, SLP, SCS, BOB, SPDR, WiBox, LTRX, or other

Note: *Ethernet device group names are not case sensitive.*

Description

Displays Ethernet devices by device group.

show ethernetdevice index

Syntax

```
show ethernetdevice index <number>
```

Description

Displays Ethernet devices by index.

show ethernetdevice list

Syntax

show ethernetdevice list

Description

Displays all Ethernet devices in short form.

show ethernetdevice port

Syntax

```
show ethernetdevice port <Device Name or IP Address> all
```

```
show ethernetdevice port <Device Name or IP Address> portnumber
<Port Number>
```

Description

Finds an Ethernet device using device name or IP address and displays port information.

show ethernetdevice search device

Syntax

```
show ethernetdevice search device <one or more parameters>
```

Parameters

```
[name <Device Name>]
```

```
[ipaddr <IP Address>]
```

```
[location <location>] [firmware <version number>]
```

Note: *Search entries are not case sensitive.*

Example

```
show ethernetdevice search device name slc firmware 4
```

Description

Displays all devices that match the criteria entered. For example, if you specify `name slc`, the SLM searches for all devices whose name starts with `slc`.

show ethernetdevice unreachablelist

Syntax

```
show ethernetdevice unreachablelist
```

Description

Displays unreachable Ethernet devices in short form.

show ethernetdevice unreachablelist index

Note: *Type `show ethernetdevice unreachablelist` to display index.*

Syntax

```
show ethernetdevice unreachablelist index <number>
```

Description

Displays unreachable ethernet devices by index.

IPv4 Filter Commands

set ipfilter delete

Syntax

set ipfilter delete <Name>

Example

```
set ipfilter delete MyFilter
```

Description

Deletes IPv4 filter set by specified name.

set ipfilter delete all

Syntax

```
set ipfilter delete all
```

Description

Deletes all references to filters.

set ipfilter delete interactive

Syntax

```
set ipfilter delete interactive
```

Description

Deletes IPv4 filters by interactive mode.

set ipfilter name delete

Note: *Type show ipfilter name <Name> or show ipfilter index <number> to display the rule number.*

Syntax

```
set ipfilter delete name <Name> [rule <rule number>]
```

Example

```
set ipfilter delete MyFilter rule 3
```

Description

Deletes IPv4 filter rule by specified name and rule number.

set ip filter state

Syntax

```
set ipfilter state <enable|disable>
```

Description

Enables or disables IPv4 filters.

set ipfilter test

Syntax

```
set ipfilter test <number of minutes>
```

Description

Enables or disables IPv4 filter test mode.

show ipfilter

Note: *Type show ipfilter to display index.*

Syntax

```
show ipfilter <parameters>
```

Parameters

```
[name <Filter Name>]
[index <number>]
```

Examples

```
show ipfilter
show ipfilter name MyFilter
show ipfilter index 2
```

Description

Displays IPv4 filter information.

show iptables

Syntax

show iptables

Description

Displays all IP filtering rules for all chains.

Logging Commands

admin locallog

Syntax

```
admin locallog clear auditlog
admin locallog clear syslog
admin locallog clear traplog device <Device Name or IP Address>
admin locallog clear traplog group <group name>
group name: SLM, SLC, SLK, SLP, SCS, LTRX, BOB, SPDR, WiBox, or
other
```

Description

Clears all of the entries in the auditlog, syslog, or traplog.

Audit Log

show auditlog

Syntax

```
show auditlog <parameters>
```

Parameters

[tail] (default)

[top]

```
[lastminutes <minutes>]
[date <MMDD>]
[date <MMDD-MMDD>]
```

Description

Lists audit log files.

show auditlog list

Syntax

show auditlog list <parameters>

Parameters

```
lastminutes <minutes>
date <MMDD>
date <MMDD-MMDD>
```

Description

Lists auditlog files in short form.

show auditlog index

Syntax

```
show auditlog index <number> <parameters>
```

`index` is the number of lines of the log specified by `lastminutes` and `date`. If you specify `0` at number of lines, all lines display.

Parameters

```
[top <number of lines>]
[tail <number of lines>]
[lastminutes <minutes>]
[date <MMDD>]
[date <MMDD-MMDD>]
[loglastminutes <minutes>]
[logdate <MMDD>]
[logdate <MMDD-MMDD>]
```

If you specify both the date and time, the SLM ignores the date.

Description

Displays the specified part of the auditlog by index.

Examples

`show auditlog`
Lists auditlog files.

`show auditlog lastminutes 5`
Lists auditlog files modified in the last 5 minutes.

`show auditlog date 0205`
Lists auditlog files last modified on 0205.

`show auditlog date 0205-0209`
Lists auditlog files last modified between 0205 and 0209.

`show auditlog index 3`
Displays index 3 from the top.

`show auditlog index 3 top 10`
Displays the first 10 lines of index 3 from the top.

`show auditlog index 3 tail 15`
Displays the last 15 lines of index 3 from the tail.

`show auditlog index 3 lastminutes 5`
Displays the lines in index 3 from the last 5 minutes of.

`show auditlog index 3 date 0205`
Displays the audit log in index 3 for the date 0205.

`show auditlog index 3 date 0205-0209`
Displays the auditlog by the index 3 between the dates 0205 to 0209.

`show auditlog index 3 top 10 lastminutes 5`
Displays the first 10 lines of index 3 of the auditlog from the last 5 minutes.

`show auditlog index 3 tail 0 lastminutes 5`
Displays all lines of the auditlog in index 3 from the tail.

`show auditlog index 3 lastminutes 5 logminutes 10`
Displays the part of auditlog in index 3 times tamped in the last 10 minutes.

`show auditlog index 3 date 0205`
Displays the part of auditlog in index 3 time- stamped on 0205.

Event Log

`show eventlog`

Syntax

`show eventlog`

Description

Lists the event log files.

Port Log

show portlog

Syntax

`show portlog`
Lists all port log files.

`show portlog <parameters>`
Lists port log files as specified by parameters.

Parameters

[lastminutes <minutes>]

[date <MMDD>]

[date <MMDD-MMDD>]

Description

Lists portlog files.

Examples

`show portlog lastminutes 5`
Lists portlog files modified in last 5 minutes.

`show portlog date 0205`
Lists portlog files last modified on 0205.

`show portlog date 0205-0209`
Lists portlog files last modified between 0205 and 0209.

show portlog file

Note: *Type* `show portlog` *to display index.*

Syntax

`show portlog file <index>`
Shows the port log from the top.

`show portlog file <index> tail`
Displays the port log from the bottom (tail).

`show portlog file <index> top`
Displays the port log from the top.

Description

Displays the contents of the portlog file by index. Default is `top`.

show portlog index

Syntax

Note: *Type* `show portlog` *to display index.*

`show portlog index <number>`
Displays part of portlog by index from the top.

Index is the number specified by `lastminutes` and date.
`show portlog index <number> <parameters>`

Parameters

`[top <number of lines>]`
Displays the part of portlog by index from the top.

`[tail <number of lines>]`
Displays the part of the portlog by index from the end.

`[lastminutes <minutes>]`

`[date <MMDD>]`

`[date <MMDD-MMDD>]`

Description

Displays the contents of the portlog file by index.

Note: *Index is the number specified by parameters* `lastminutes` *and* `date`*. If you specify* `0` *as number of lines, all lines display. If you specify both date and time, the SLM ignores the date option.*

Examples

`show portlog index 3`
Displays the specified portlog from top.

`show portlog index 3 top 10`
Displays the first 10 lines of specified portlog from top.

`show portlog index 3 tail 15`
Displays the last 15 lines of specified port log from tail.

`show portlog index 3 lastminutes 5`
Displays port log by the index '3'.
To get this index, type `show portlog lastminutes 5`.

`show portlog index 3 date 0205`
Displays port log by the index '3'.
To get this index, type `show portlog date 0205`.

`show portlog index 3 date 0205-0209`
Displays port log by the index '3'.
To get this index, type `show portlog date 0205-0209`.

`show portlog index 3 top 10 lastminutes 5`
Displays the first 10 lines of portlog by the index '3'.
To get this index, type `show portlog lastminutes 5`.

`show portlog index 3 tail 0 lastminutes 5`
Displays the portlog by the index '3' from tail.
To get this index, type `show portlog lastminutes 5`.

show portlog list

Syntax

`show portlog list`

`show portlog list <parameters>`

Parameters

`[lastminutes <minutes>]`

`[date <MMDD>]`

`[date <MMDD-MMDD>]`

Description

Lists portlog files in short form.

Session Log

show sessionlog

Syntax

```
show sessionlog type <sessiontype> <parameters>
```

```
sessiontype: <slcportactive|slcportsaved|scsport|device>
```

Parameters

```
[lastminutes <minutes>]
```

```
[date <MMDD>]
```

```
[date <MMDD-MMDD>]
```

Description

Lists session log files.

Examples

`show sessionlog`
Lists device session log files.

`show sessionlog type slcportsaved lastminutes 5`
Lists archived SLC port session log files modified in last 5 minutes.

`show sessionlog date 0205`
Lists session log files last modified on 0205.

`show sessionlog type scsport index 3`
Displays the specified SCS05/20 port session log from the top.

`show sessionlog type device index 3 top 10`
Displays the first 10 lines of the specified device session log from the top.

`show sessionlog type device index 3 tail 15`
Displays the last 15 lines of specified device session log from the end.

`show sessionlog type device index 3 lastminutes 5`
Displays device session log by the index '3'.
To get this index, type `show portlog lastminutes 5`.

`show sessionlog type slcportsaved index 3 date 0205`
Displays archived SLC port sessionlog by the index '3'.
To get this index, type `show sessionlog type slcportsaved date 0205`.

`show sessionlog type device index 3 date 0205-0209`
Displays device session log by the index '3'.
To get this index, type `show sessionlog type device date 0205-0209`.

`show sessionlog type device index 3 top 10 lastminutes 5`
Displays the first 10 lines of device session log by the index '3'.
To get this index, type `show sessionlog type device lastminutes 5`.

System Log

show syslog

Syntax

show syslog <parameters>

Parameters

[tail] (default)

[top]

[lastminutes <minutes>]

[date <MMDD>]

[date <MMDD-MMDD>]

Description

Lists syslog files.

show syslog list

Syntax

show syslog list <parameters>

Parameters

lastminutes <minutes>

date <MMDD>

date <MMDD-MMDD>

Description

Lists syslog files in short form.

show syslog index

Syntax

show syslog index <number> <parameters>
index is the number of lines of the log specified by lastminutes and date. If you specify 0 at number of lines, all lines display.

Parameters

[top <number of lines>]

[tail <number of lines>]

[lastminutes <minutes>]

[date <MMDD>]

[date <MMDD-MMDD>]

[loglastminutes <minutes>]

[logdate <MMDD>]

[logdate <MMDD-MMDD>]

If you specify both the date and time, the SLM ignores the date.

Description

Displays the specified part of the syslog by index.

Examples

`show syslog`
Lists syslog files.

`show syslog lastminutes 5`
Lists syslog files modified in the last 5 minutes.

`show syslog date 0205`
Lists syslog files last modified on 0205.

`show syslog date 0205-0209`
Lists syslog files last modified between 0205 and 0209.

`show syslog index 3`
Displays index 3 from the top.

`show syslog index 3 top 10`
Displays the first 10 lines of index 3 from the top.

`show syslog index 3 tail 15`
Displays the last 15 lines of index 3 from the tail.

`show syslog index 3 lastminutes 5`
Displays the lines in index 3 from the last 5 minutes of.

`show syslog index 3 date 0205`
Displays the audit log in index 3 for the date 0205.

`show syslog index 3 date 0205-0209`
Displays the syslog by the index 3 between the dates 0205 to 0209.

`show syslog index 3 top 10 lastminutes 5`
Displays the first 10 lines of index 3 of the syslog from the last 5 minutes.

`show syslog index 3 tail 0 lastminutes 5`
Displays all lines of the syslog in index 3 from the tail.

`show syslog index 3 lastminutes 5 logminutes 10`
Displays the part of syslog in index 3 time- stamped, in the last 10 minutes.

`show syslog index 3 date 0205`
Displays the part of syslog in index 3 time stamped, on 0205.

Trap Log

`show traplog`

Syntax

`show traplog <parameters>`

Parameters

[tail] (default)

[top]

`[lastminutes <minutes>]`

`[date <MMDD>]`

`[date <MMDD-MMDD>]`

Description
Lists traplog files.

show traplog group
Note: Type `show traplog group` to display the index.

Syntax
```
show traplog group <Device Group Name> [index <number>]
```
Group name: SLM, SLC, SLK, SLP, SCS, LTRX, or other

Description
Displays the current trap log information for an Ethernet device group by index number.

show traplog list

Syntax
```
show traplog list <parameters>
```

Parameters
```
lastminutes <minutes>
date <MMDD>
date <MMDD-MMDD>
```

Description
Lists traplog files in short form.

show traplog index

Syntax
```
show traplog index <number> <parameters>
```
`index` is the number of lines of the log specified by `lastminutes` and `date`. If you specify `0` at number of lines, all lines display.

Parameters
```
[top <number of lines>]
[tail <number of lines>]
[lastminutes <minutes>]
[date <MMDD>]
[date <MMDD-MMDD>]
[loglastminutes <minutes>]
[logdate <MMDD>]
[logdate <MMDD-MMDD>]
```
If you specify both the date and time, the SLM ignores the date.

Description
Displays the specified part of the traplog by index.

Examples
```
show traplog
```
Lists traplog files.

`show traplog lastminutes 5`
Lists traplog files modified in the last 5 minutes.

`show traplog date 0205`
Lists traplog files last modified on 0205.

`show traplog date 0205-0209`
Lists traplog files last modified between 0205 and 0209.

`show traplog index 3`
Displays index 3 from the top.

`show traplog index 3 top 10`
Displays the first 10 lines of index 3 from the top.

`show traplog index 3 tail 15`
Displays the last 15 lines of index 3 from the tail.

`show traplog index 3 lastminutes 5`
Displays the lines in index 3 from the last 5 minutes of.

`show traplog index 3 date 0205`
Displays the audit log in index 3 for the date 0205.

`show traplog index 3 date 0205-0209`
Displays the traplog by the index 3 between the dates 0205 to 0209.

`show traplog index 3 top 10 lastminutes 5`
Displays the first 10 lines of index 3 of the traplog from the last 5 minutes.

`show traplog index 3 tail 0 lastminutes 5`
Displays all lines of the traplog in index 3 from the tail.

`show traplog index 3 lastminutes 5 logminutes 10`
Displays the part of traplog in index 3 times tamped in the last 10 minutes.

`show traplog index 3 date 0205`
Displays the part of traplog in index 3 times stamped on 0205.

Maintenance Commands

admin config

Syntax

`admin config factorydefaults`

Description

Restores the SLM configuration and device database settings to factory defaults.

admin config rebuilddatabase

Syntax

`admin config rebuilddatabase`

Description

Removes and rebuilds the SLM configuration and database from scratch, in case of database corruption that cannot be fixed by the factory.

admin config showfiles

Syntax

```
admin config showfiles
```

Description

Shows saved configuration files.

admin config save file

Syntax

```
admin config save file <filename>
```

Description

Saves the SLM configuration to the SLM Configuration Files directory.

admin locallog clear

Syntax

```
admin locallog clear auditlog
admin locallog clear syslog
admin locallog clear traplog device <Device Name or IP Address>
admin locallog clear traplog group <group name>
group name: SLM, SLC, SLK, SLP, SCS, LTRX, BOB, SPDR, WiBox, or other
```

Description

Clears all of the entries in the auditlog, syslog, or traplog.

admin quicksetup

Syntax

```
admin quicksetup
```

Description

Displays the quick setup script on the CLI; only the sysadmin account can use this command.

admin reboot

Syntax

```
admin reboot
```

Description

Terminates all connections and reboots the SLM.

admin securechannel regenkey

Syntax

```
admin securechannel regenkey
```

Description

Regenerates the secure channel key.

Note: With this command, you lose access to established secure channels; therefore, the SLM first requests confirmation that you want to regenerate the securechannel key.

admin shutdown

Syntax

```
admin shutdown
```

Description

Terminates all connections, shuts down the SLM, and turns off the power.

admin version

Syntax

```
admin version
```

Description

Displays current application version information.

show progress

Syntax

```
show progress
```

Description

Shows the progress of background tasks.

show sysconfig

Syntax

```
show sysconfig [email <Email Address>]
```

Description

Displays a report of configurable parameters. The output can be emailed.

Managed Devices

Administrators, Ethernet Account Users and Menu Only Users

set manageddevice config

Syntax

```
set manageddevice config <Device Name> <one or more parameters>
```

Parameters

```
name <New Name>
powerport <1|2> state <on|off|cyclepower>]
[dialout <Dial Account Name|enable|disable>
modem <Modem Name>
```

To set modem parameters, you must specify the dial-out option.

```
phonenumber <phone number>]
```

```
application <ssh|telnet|http|none>]
```

Examples

```
set ma config port-1 name waimea-port-1
```
Specifies a managed device name (port-1) and renames it to waimea-port-1.

```
set ma config slp-sunset-port1 state off
```
Specifies a managed device name (slp-sunset-port1) and turns the power off.

Description

Finds a managed device-by-device name and modifies device parameters.

set manageddevice index

Note: *Type* `show manageddevice` *all to display index.*

Syntax

```
set manageddevice index <number> <one or more parameters>
```

Parameters

```
name <New Name>
```

```
powerport <1|2> state <on|off|cyclepower> (SLP only)
```

```
delete
```

```
dialout <Dial Account Name|enable|disable>
```

```
modem <Modem Name>
```
To set modem parameters, you must specify the dial-out option.

```
phonenumber <phone number>
```

```
application <ssh|telnet|http|none>
```

Examples

```
set ma config port-1 name waimea-port-1
```

```
set ma config slp-sunset-port1 powerport 1 state off
```

```
set ma index 1 delete
```

```
set ma index 1 dialout myaccount modem pci-s4 phone 3334444
```

If you set `dialout myaccount first` and then decide to set `modem` and `phonenumber` later, you still must specify `dialout myaccount` or `dialout enable`.

```
set ma index 1 dialout myaccount
```

```
set ma index 1 dialout enable modem pci-s4 phone 3334444
```

Description

Finds managed device by index and modifies device parameters.

set manageddevice config <Device Name> disconnect modem

Syntax

```
set manageddevice config <Device Name> disconnect modem
```

Description

Finds managed device by name and disconnects modem.

set manageddevice index <number> disconnect modem

Note: *Type* `show manageddevice all` *to display index.*

Syntax

```
set manageddevice index <number> disconnect modem
```

Example

```
set ma index 2 disconnect modem
```

Description

Finds managed device by index number and disconnects modem.

show device

Syntax

Note: *Entries are not case sensitive.*

```
show device <device name>
```

Description

Searches for and displays Ethernet or managed devices by device name. For example, if you specify `name slc`, the SLM searches for all Ethernet and managed devices whose name starts with `slc`.

show device all

Syntax

```
show device all
```

```
show device
```

Description

Displays all Ethernet and managed devices.

show manageddevice all

Syntax

```
show manageddevice all
```

```
show manageddevice
```

Description

Displays information about all managed devices.

show manageddevice config

Syntax

```
show manageddevice config <Device Name>
```

Description

Displays the configuration of a managed device.

show manageddevice index

Note: *Type* `show manageddevice all` *to display index.*

Syntax

show manageddevice index <number>

Description

Displays managed devices by index.

show manageddevice list

Syntax

show manageddevice list

Description

Displays all managed devices in short form.

show manageddevice search

Syntax

```
show manageddevice search <one or more parameters>
```

Parameters

Note: *Search entries are not case sensitive.*

```
[name <Port Name>]
```

Example

```
show manageddevice search name waimea-port
```

Description

Displays all ports that match the criteria entered.

Managed Device Users

set manageddevice config

Syntax

```
set manageddevice config <Device Name> <one or more parameters>
```

Parameters

```
[name <New Name>]
```

```
[state <on|off|cyclepower>]
```
(available for SLP only)
Powers managed device on or off.

Examples

```
set ma config port-1 name waimea-port-1
```
Specifies a managed device name (port-1) and renames it to waimea-port-1.

```
set ma config slp-sunset-port1 state off
```
Specifies a managed device name (slp-sunset-port1) and turns the power off.

Description

Finds a managed device-by-device name and modifies device parameters.

set manageddevice index

Note: Type `show manageddevice` *all to display index.*

Syntax

```
set manageddevice index <number> <one or more parameters>
```

Parameters

```
name <New Name>
powerport <1|2> state <on|off|cyclepower>] (SLP only)
```

Example

```
set ma port slp-sunset po 2 state on
```

Description

Finds managed device by index and modifies device parameters.

set manageddevice config <Device Name> disconnect modem

Syntax

```
set manageddevice config <Device Name> disconnect modem
```

Description

Finds managed device by name and disconnects modem.

set manageddevice index <number> disconnect modem

Note: Type `show manageddevice all` *to display index.*

Syntax

```
set manageddevice index <number> disconnect modem
```

Example

```
set ma index 2 disconnect modem
```

Description

Finds a managed device by index number and disconnects modem.

Menu Commands

Users can have custom user menus as their command line interface rather than the standard CLI command set. Each custom user menu can contain up to 50 commands (`logout` is always the last command). Instead of typing each command, the user enters the number associated with the command. Each command can also have an associated nickname that can be displayed in the menu instead of the command. You can use the `showmenu <Menu Name>` and `returnmenu` commands to display another menu from a menu or to return to the prior menu.

set menu add

Syntax

```
set menu add <Menu Name> [command <command number>]
```

Description

Creates a new custom user menu or adds a command to an existing custom user menu.

set menu delete

Syntax

```
set menu delete <Menu Name> [command <command number>]
```

Description

Deletes a custom user menu or one command within a custom user menu.

set menu edit

Syntax

```
set menu edit <Menu Name> command <command number>
```

Changes a command within an existing custom user menu.

```
set menu edit <Menu Name> nickname <command number>
```

Changes a nickname within an existing custom user menu.

```
set menu edit <Menu Name> title <menu title>
```

Sets the optional title for a menu.

```
set menu edit <Menu Name> shownicknames <enable|disable>
```

Enables or disables display of command nicknames instead of commands.

```
set menu edit <Menu Name> redisplaymenu <enable|disable>
```

Enables or disables redisplay of menu before each prompt.

Description

Changes menu properties.

show menu

Syntax

```
show menu <Menu Name>
```

```
show menu name <Menu Name>
```

```
show menu all
```

Description

Shows a list of all menu names or all commands for a specific menu.

Note: *To see assignments to account group, type* `help show accountgroup`.

Modem Commands

reset modem connection

Note: *You may only use this command when the modem is completely stuck.*

Wait for minimum timeout period (3 minutes) before you use this command when:

- *You dial out via PPP and encounter no dial tone.*
- *You dial out via PPP and encounter a busy signal.*

Syntax

```
reset modem connection
```

Description

Resets a modem connection.

set modem scan

Syntax

```
set modem scan
```

Description

Scans a modem.

set modem disconnect

Note: *Type* `show modem` *to view the current modem connections.*

Syntax

```
set modem disconnect <Name>
```

Example

```
set modem disconnect MyPCIModem
```

Description

Terminates modem dial-out connection.

set modem edit

Syntax

```
set modem edit <Modem Name> <parameters>
```

Parameters

`name <New Name>`

`baud <300-115200>`

`flowcontrol <none|xon/xoff|rts/cts>`

`initscript <Modem Initialization Script>`

`defaultinitscript <Modem Default Initialization Script>`

`dialin <Dial Account Name|CLEAR|disable|enable>`

`CLEAR` removes the dial account assignment.

`disable` disables dial-in.

`enable` enables dial-in

`ipfilter <IPv4 Filter Name|CLEAR>`

`ipfilter CLEAR` removes the ipfilter assignment.

Description

Configures a currently loaded modem.

show modem

Syntax

```
show modem
```

Description

Displays all modems.

show modem connection

Syntax

show modem connection <parameters>

Parameters

[index <number>]

Description

Displays active (established) modem connections.

show modem settings

Syntax

show modem <parameters>

Parameters

[name <Modem Name>]

[index <number>]

Description

Displays modem settings.

show modem status

Syntax

show modem status

Description

Displays the status of the modem.

Network Commands

admin quicksetup

Syntax

admin quicksetup

Description

Displays the quick setup script on the CLI; only the sysadmin account can use this command.

set network bonding

Syntax

set network bonding <disabled|active-backup|802.3ad-2|802.3ad-34|adaptive-balancing>

Description

Configures Ethernet bonding.

set network dns

Syntax

```
set network dns <1|2|3> ipaddr <IP Address>
```

Description

Configures up to three DNS servers.

set network gateway

Syntax

```
set network gateway <parameters>
```

Parameters

```
default <IP Address>
precedence <dhcp|default>
alternate <IP Address>
pingip <IP Address>
ethport <1 or 2>
pingdelay <1-250 seconds>
failedpings <1-250>
```

Description

Sets the default gateway.

set network host

Syntax

```
set network host <Hostname>
```

Description

Sets the SLM hostname.

set network port

Syntax

```
set network port <1|2> <parameters>
```

Parameters

```
state <dhcp|bootp|static|disable>
[ipaddr <IP Address> mask <Mask>]
mode <auto|10mbit-half|100mbit-half|10mbit-full|100mbit-full>
[ipfilter <IPv4 Filter Name | CLEAR>]
```

`CLEAR` removes the IP filter assignment.

Description

Configures Network Port 1 or 2.

show network all

Syntax

```
show network all
```

Description

Displays all network settings.

show network bonding

Syntax

```
show network bonding
```

Description

Displays network bonding information.

show network port

Syntax

```
show network port <1|2>
```

Description

Displays Network Port 1 and Network Port 2 connection information.

show network settings

Syntax

```
show network settings
```

Description

Displays all network settings.

Port Commands

set ethernetdevice port

Syntax

```
set ethernetdevice port <Device Name or IP Address> portnumber
<port number or list> <one or more parameters>
```

Parameters

`[name <New Port Name>]`

`[state <on|off|cyclepower>]` (available for SLP only)
Powers Ethernet device port on or off.

Note: *Only SLP outlet action supports a port list.*

Examples

To power up SLP outlet 2:

```
set eth port slp-sunset po 2 state on
```

To power up SLP outlet port list 1-3,6,8-14

```
set eth port slp-sunset po 1-3,6,8-14 state on
```

Description

Finds a port by device name or IP address with the port number and modifies port parameters.

show ethernetdevice port

Syntax

```
show ethernetdevice port <Device Name or IP Address> all
```

```
show ethernetdevice port <Device Name or IP Address> portnumber <Port Number>
```

Description

Finds an Ethernet device using device name or IP address and displays port information.

show ethernetdevice search port

Syntax

```
show ethernetdevice search port <one or more parameters>
```

Parameters

Note: *Search entries are not case sensitive.*

```
[name <Port Name>]
```

```
[portnumber <Port Number>]
```

Examples

```
show ethernetdevice search port name waimea-port
```

```
show ethernetdevice search port name waimea portnumber 2
```

Description

Displays all ports that match the criteria entered.

show port

Note: *Type* `show port all` *to display index.*

Syntax

```
show port <name>
```

Example

`show port slc` displays all Ethernet ports whose name starts with "slc."

Description

Searches Ethernet ports by port name and displays port information.

show port all

Syntax

```
show port all
```

```
show port
```

Displays all Ethernet ports.

show port index

Syntax

`show port index <number>`

Description

Displays Ethernet ports by index.

Search Commands

show account search email

Syntax

show account search email <email address>

Example

`show account search email sys`

Displays all accounts whose email address starts with "sys."

Description

Displays accounts that match the email address entered.

show account search name

Syntax

`show account search name <user name>`

Examples

`show account search name sys`

Displays all accounts whose name starts with "sys."

Description

Displays accounts that match the name entered.

show ethernetdevice search device

Syntax

`show ethernetdevice search device <one or more parameters>`

Parameters

Note: *Search entries are not case sensitive.*

`[name <Device Name>]`

`[ipaddr <IP Address>]`

`[location <location>] [firmware <version number>]`

Example

`show ethernetdevice search device name slc firmware 4`

Description

Displays all devices that match the criteria entered. For example, if you specify `name slc`, the SLM searches for all devices whose name starts with `slc`.

show ethernetdevice search port

Syntax

```
show ethernetdevice search port <one or more parameters>
```

Parameters

Note: *Search entries are not case sensitive.*

```
[name <Port Name>]
[portnumber <Port Number>]
```

Examples

```
show ethernetdevice search port name waimea-port
show ethernetdevice search port name waimea portnumber 2
```

Description

Displays all ports that match the criteria entered.

show manageddevice search

Syntax

```
show manageddevice search <one or more parameters>
```

Parameters

Note: *Search entries are not case sensitive.*

```
[name <Port Name>]
```

Examples

```
show manageddevice search name waimea-port
```

Description

Displays all ports that match the criteria entered.

Services Commands

set service auditlog

Syntax

```
set service auditlog <enable|disable>
```

Description

Enables or disables audit logging.

set service https

Syntax

```
set service https <enable|disable>
```

Description

Enable or disables HTTPS.

set service telnet

Syntax

```
set service telnet <enable|disable>
```

Description

Enables or disables Telnet logging to the SLM.

set service sessionlog

Syntax

```
set service sessionlog <enable|disable>
```

Description

Enables or disables session logging.

set service ssh

Syntax

```
set service ssh <enable|disable> version <1|2>
```

Description

Enables or disables SSH logging to the SLM.

set service wap

Syntax

```
set service wap <enable|disable>
```

Description

Enables or disables WAP access to SLM.

show service

Syntax

```
set service
```

Description

Displays service settings.

Session Commands

connect terminate

Syntax

```
connect terminate <connect ID> <one or more parameters>
```

Parameters

```
outbound <outbound ID>
```

You must specify connection ID (inbound ID) to terminate an outbound connection.

Use `show connection` to view the current connections and their ID.

Examples

```
connect terminate 3
connect terminate 3 outbound 1
```

Description

Terminates a user connection to the SLM session. Use `show connection` to view the current connections and IDs.

show connection

Syntax

```
show connection
```

Description

Displays active user connections and connection IDs.

SSH Key Commands

set sshkey delete

Syntax

```
set sshkey delete keyuser <SSH Key User> keyhost <SSH Key Host>
```

Description

```
Deletes an imported SSH key.
```

set sshkey import

Syntax

```
set sshkey import <copypaste>
```

Note: RSA keys must be 1024 bits

Description

Imports an SSH key.

show sshkey import

Syntax

```
show sshkey import <one or more parameters>
```

Parameters

```
[keyuser <SSH Key User>]
[keyhost <SSH Key IP Address or Name>]
[viewkey <enable|disable>]
```

Description

Displays imported SSH keys.

Task Progress Command

show progress

Syntax

```
show progress
```

Description

Shows the progress of background tasks.

B: Security Considerations

The SLM provides data path security by means of SSH, Web/SSL, and in the case of SLCs, secure channel. Even with the use of these protocols, however, do not assume you have complete security. Securing the data path is only one measure needed to ensure security. This appendix briefly discusses some important security considerations.

Security Practice

Develop and document a Security Practice. The Security Practice should state:

- The dos and don'ts of maintaining security. For example, the power of SSH and SSL is compromised if users leave sessions open or advertise their password.
- The assumptions that users can make about the facility and network infrastructure, for example, how vulnerable the CAT 5 wiring is to tapping.

Factors Affecting Security

External factors affect the security provided by the SLM, for example:

- A terminal to the SLM may be secure, but the path from the SLM to the end device may not be secure.
- With the right tools, a person having physical access to open the SLM may be able to read the encryption keys.
- There is no true test for a denial-of-service attack—there is always a legitimate scenario for a request storm. A denial-of-service filter locks out some high-performance automated/scripted requests. The SLM attempts to service all requests and does not filter out potential denial–of-service attacks.

Available Services and Port Numbers

The SLM supports the services listed below. When installing and configuring an SLM in an environment where such services are limited, please make sure network equipment configurations allow access to and from the listed port numbers.

Administration

Protocol	Port#	Type
SSH	22	TCP
HTTP	80	TCP
HTTPS (SSL)	443	TCP
Telnet	23	TCP

Management

Protocol	Port#	Type
SMTP	25	TCP
BOOTP/DHCP	67/68	TCP
NTP	123	TCP
NIS	111	TCP/UDP
SNMP	161/162	UDP
LDAP	389	TCP
RADIUS	1645/1812	TCP/UDP

Device Access

Protocol	Port#	Type
FTP	20/21	TCP/UDP
SSH/SCP	22	TCP
TFTP	69	UDP
SNMP	161/162	UDP
LDP	30718	UDP

C: Safety Information

Safety Precautions

Please follow the safety precautions described below when installing and operating the SLM.

Cover

- Do not remove the cover of the chassis. There are no user-serviceable parts inside. Opening or removing the cover may expose you to dangerous voltage that could cause fire or electric shock.
- Refer all servicing to Lantronix.

Power Plug

- When disconnecting the power cable from the socket, pull on the plug, not the cord.
- Always connect the power cord to a properly wired and grounded power source. Do not use adapter plugs or remove the grounding prong from the cord.
- Only use a power cord with a voltage and current rating greater than the voltage and current rating marked on the unit.
- Install the unit near an AC outlet that is easily accessible.
- Always connect any equipment used with the product to properly wired and grounded power sources.
- To help protect the product from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Do not connect or disconnect this product during an electrical storm.

Input Supply

- Disconnect all power supply sources before servicing to avoid electric shock.
- Check nameplate ratings to assure there is no overloading of supply circuits that could affect overcurrent protection and supply wiring.

Grounding

- Maintain reliable grounding of this product.
- Pay particular attention to supply connections when connecting to power strips rather than directly to the branch circuit.

Rack

If rack mounted units are in a closed or multi-unit rack assembly, they may require further evaluation by Certification Agencies. Consider the following:

- Do **not** install the unit in a rack in such a way that a hazardous stability condition results because of uneven loading. A drop or fall could cause injury.
- The ambient temperature inside the rack may be greater than the room ambient temperature. Make sure to install the SLM in an environment with an ambient temperature less than the maximum operating temperature of the SLM. (See *D: Technical Specifications*.)
- Install the equipment in a rack in such a way that the amount of airflow required for safe operation of the equipment is not compromised.
- Mount the equipment in the rack so that a hazardous condition is not achieved due to uneven mechanical loading.
- Maintain reliable earthing of rack-mounted equipment. Give particular attention to supply connections other than direct connections to the branch circuit (e.g., use of power strips).
- Before operating the SLM, make sure the SLM is secured to the rack.

Port Connections

- Only connect the network ports to an Ethernet network that supports 10Base-T/100Base-T or 10/100/1000Base-T.
- Only connect the console port to equipment with serial ports that support EIA-232 (formerly RS-232C).

D: Technical Specifications

You can install the SLM either in an EIA-standard 19-inch rack (1U tall) or as desktop unit. Following are specifications for the SLM-01 and the SLM-02.

	SLM-01	SLM-02
Memory	40 GB Hard Drive 256 MB RAM	160 GB Hard Drive 512 MB RAM
Network interface	One 10/100Base-T (RJ45) One 10/100/1000Base-T (RJ45)	Two 10/100/1000Base-T (RJ45)
Dimensions	1U, 43 x 429 x 584 mm (1.7 H x 16.9 x 23 in)	1U, 44 x 424 x 356 mm (1.7 H x 16.7 x 14 in)
Weight	12.7 kg (28 lb)	10.5 kg (23 lb)
Console	RS-232 (DB9)	RS-232 (DB9)
Power Supply	100-240 VAC 50 -60 Hz	100-240 VAC 50 -60 Hz
Temperature	Operating: 10°C to 35°C (50°F to 95°F) Storage: -40°C to + 70°C (140°F to 158°F)	Operating: 10°C to 35°C (50°F to 95°F) Storage: -40°C to + 70°C (140°F to 158°F)
Relative Humidity	Operating: Non-Operating/Storage: 95%, non-condensing at 30^0C	Operating: Non-Operating/Storage: 95%, non-condensing at 30^0C

E: Compliance Information

SLM-01

(according to ISO/IEC Guide 22 and EN 45014)

Manufacturer's Name & Address:

Lantronix Inc., 15353 Barranca Parkway, Irvine, CA 92618 USA

Declares that the following product:

Product Name(s): Model SecureLinx Management Appliance (SLM)

Conform to the following standards or other normative documents:

Safety:

UL/CSA 60950-1:2003
EN60950
CE Mark EU Directive 73/23/EEC, IEC
IEC 60 950
EMKO-TSE (74-SEC) 207/94
GOST-R 50377-92 (GOST-R Mark)

Electromagnetic Immunity:

FCC Class A	AS/NZS 3548 Class A (C-tick Mark)
ICES-003 Class A	RRL Class A Certification to MIC Notices 1997-41 & 1997-42
EN55022 Class A	GOST-R 29216-91
EN55024 (Immunity)	GOST-R 50628-95 (GOST-R Mark)
CE Mark (EU Directive 89/336/EEC)	BSMI CNS13438 Class A (DOC
CISPR-22/VCCI Class A	

Supplementary Information:

This Class A digital apparatus complies with ICES-003 (Class A), EN55022 Class A

EN55024 (immunity) and has been verified as being compliant within the Class A limits of the FCC Radio Frequency Device Rules (FCC Title 47, Part 15, Subpart B CLASS A), measured to CISPR 22: 1993 limits and methods of measurement of Radio Disturbance Characteristics of Information Technology Equipment. The product complies with the requirements of the Low Voltage Directive 72/23/EEC and the EMC Directive 89/336/EEC.

Additional Agency Approvals and Certifications:

VCCI	C-Tick
TUV	CB Scheme
GS Mark	NIST-certified implementation of AES as specified by FIPS 197
UL/CUL	

This product carries the **CE** mark since it has been tested and found compliant with the following standards:

Safety:	EN 60950
Emissions:	EN 55022 Class A
Immunity:	EN 55024

Manufacturer's Contact:

Director of Quality Assurance, Lantronix Inc.	Phone: 949-453-3990
15353 Barranca Parkway, Irvine, CA 92618 USA	Fax: 949-453-3995

SLM-02

(according to ISO/IEC Guide 22 and EN 45014)

Manufacturer's Name & Address:

Lantronix Inc., 15353 Barranca Parkway, Irvine, CA 92618 USA

Declares that the following product:

Product Name(s): Model SecureLinx Management Appliance (SLM)

Conform to the following standards or other normative documents:

Safety:

UL 60950
EN 60950
CE Mark EU Directive 73/23/EEC, IEC
IEC 60950

Electromagnetic Immunity:

FCC Class B
EN61000-3-2/3-3
EN55022 Class B
EN55024 (Immunity)
CE Mark (EU Directive 89/336/EEC)
CISPR-22 Class B

CISPR-24

Supplementary Information:

This Class B digital apparatus complies with EN55022 Class B

EN55024 (immunity) and has been verified as being compliant within the Class B limits of the FCC Radio Frequency Device Rules, measured to CISPR 22.

Additional Agency Approvals and Certifications:

TUV

UL/CUL

This product carries the **CE** mark since it has been tested and found compliant with the following standards:

Safety:	EN 60950
Emissions:	EN 55022 Class B
Immunity:	EN 55024

Manufacturer's Contact:

Director of Quality Assurance, Lantronix Inc.
15353 Barranca Parkway, Irvine, CA 92618
USA

Phone: 949-453-3990
Fax: 949-453-3995

F: Protocol Glossary

This glossary provides brief definitions of commonly used protocols.

BOOTP (Bootstrap Protocol)

Similar to DHCP, but for smaller networks. Automatically assigns the IP address for a specific duration of time.

CHAP (Challenge Handshake Authentication Protocol)

A secure protocol for connecting to a system; it is more secure than the PAP.

DHCP (Dynamic Host Configuration Protocol)

Internet protocol for automating the configuration of computers that use TCP/IP.

DNS (Domain Name Servers): A system that allows a network nameserver to translate text host names into numeric IP addresses.

Kerberos

A network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography.

LDAP (Lightweight Directory Access Protocol)

A protocol for accessing directory information.

NAT (Network Address Translation)

An Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. This enables a company to shield internal addresses from the public Internet.

NFS (Network File System)

A protocol that allows file sharing across a network. Users can view, store, and update files on a remote computer. You can use NFS to mount all or a portion of a file system. Users can access the portion mounted with the same privileges as the user's access to each file.

NIS (Network Information System)

System developed by Sun Microsystems for distributing system data such as user and host names among computers on a network.

NMS (Network Management Station)

NMS acts as a central server, requesting and receiving SNMP-type information from any computer using SNMP.

NTP (Network Time Protocol)

A protocol used to synchronize time on networked computers and equipment.

PAP (Password Authentication Protocol)

A method of user authentication in which the username and password are transmitted over a network and compared to a table of name-password pairs.

PPP (Point-to-Point Protocol)

A protocol for creating and running IP and other network protocols over a serial link.

RADIUS (Remote Authentication Dial-In User Service)

An authentication and accounting protocol. Enables remote access servers to communicate with a central server to authenticate dial-in users and their access permissions. A company stores user profiles in a central database that all remote servers can share.

Secure Channel

The name that Lantronix gave to encrypted password-less connections on the SLM. These connections use public key encryption for authentication over SSH.

SecurID

SecurID is a two-factor authentication method based on the user's SecurID token and pin number.

SMB/CIFS

(Server Message Block/Common Internet File System): Microsoft's protocol for allowing all applications as well as Web browsers to share files across the Internet. CIFS runs on TCP/IP and uses the SMB protocol in Microsoft Windows for accessing files. With CIFS, users with different platforms and computers can share files without having to install new software.

SNMP (Simple Network Management Protocol)

A protocol that administrators use to monitor networks and connected devices and to respond to queries from other network hosts.

SMTP (Simple Mail Transfer Protocol)

TCP/IP protocol for sending email between servers.

SSL (Secure Sockets Layer)

A protocol that provides authentication and encryption services between a web server and a web browser.

SSH (Secure Shell)

A secure transport protocol based on public-key cryptography.

TACACS+ (Terminal Access Controller Access Control System)

A method of authentication used in UNIX networks. It allows a remote access server to communicate with an authentication server to determine whether the user has access to the network.

G: Warranty

Lantronix warrants each Lantronix product to be free from defects in material and workmanship for a period of **TWO YEARS** after the date of shipment. During this period, if a customer is unable to resolve a product problem and Lantronix Technical Support determines the product is defective, a Return Material Authorization (RMA) will be issued. Following receipt of an RMA number, the customer shall return the product to Lantronix, freight prepaid. Upon verification of warranty, Lantronix will -- at its option -- repair or replace the product and return it to the customer freight prepaid. If the product is not under warranty, the customer may have Lantronix repair the unit on a fee basis or return it. No services are handled at the customer's site under this warranty. This warranty is voided if the customer uses the product in an unauthorized or improper way, or in an environment for which it was not designed.

Lantronix warrants the media containing its software product to be free from defects and warrants that the software will operate substantially according to Lantronix specifications for a period of **60 DAYS** after the date of shipment. The customer will ship defective media to Lantronix. Lantronix will ship the replacement media to the customer.

* * * *

In no event will Lantronix be responsible to the user in contract, in tort (including negligence), strict liability or otherwise for any special, indirect, incidental or consequential damage or loss of equipment, plant or power system, cost of capital, loss of profits or revenues, cost of replacement power, additional expenses in the use of existing software, hardware, equipment or facilities, or claims against the user by its employees or customers resulting from the use of the information, recommendations, descriptions and safety notations supplied by Lantronix. Lantronix liability is limited (at its election) to:

Refund of buyer's purchase price for such affected products (without interest)

Repair or replacement of such products, provided that the buyer follows the above procedures.

There are no understandings, agreements, representations or warranties, express or implied, including warranties of merchantability or fitness for a particular purpose, other than those specifically set out above or by any existing contract between the parties. Any such contract states the entire obligation of Lantronix. The contents of this document shall not become part of or modify any prior or existing agreement, commitment, or relationship.

For details on the Lantronix warranty replacement policy, please go to our web site at http://www.lantronix.com/support/warranty/index.html